Evaluación del Rendimiento de una Solución de Cupones Electrónicos para Dispositivos Móviles

Andreu Pere Isern-Deyà, M. Francisca Hinarejos, Josep Lluís Ferrer-Gomila
Universitat de les Illes Balears (UIB), Email: {andreupere.isern, xisca.hinarejos, jlferrer}@uib.es

***Resumen*—El comercio electrónico móvil (m-commerce) representa ya una importante área de negocio con grandes oportunidades para consumidores y comerciantes. Sin embargo, todavía existen escenarios que requieren mejoras en cuanto a eficiencia, como son los cupones electrónicos. La eficiencia y el rendimiento de estas soluciones suele medirse únicamente considerando el coste de las operaciones criptográficas o realizando pruebas de laboratorio en entornos limitados, muchas veces una única máquina para ejecutar todo el escenario de pruebas (incluyendo consumidores y comerciantes). En este artículo presentamos un análisis del rendimiento de una solución de cupones electrónicos, mediante la cual comprobamos que no es suficiente analizar únicamente la carga debido a las operaciones criptográficas, sino que también deben considerarse otros factores, como el efecto de la red.**

***Index Terms*—cupón electrónico, seguridad, privacidad, eficiencia, análisis de rendimiento**

I. Introducción

El comercio electrónico (e-commerce) representa uno de los sectores más dinámicos e innovadores dentro de la economía global. Hoy día la atención que recibe el e-commerce es incluso mayor dado el auge de los dispositivos móviles y la mejora de las infraestructuras móviles de comunicaciones. De hecho, la cuota de mercado de usuarios con teléfonos inteligentes ha alcanzado alrededor del 18 % del total de dispositivos de usuario [1], siendo el comercio móvil (m-commerce) uno de los sectores más beneficiados por este hecho. De acuerdo con predicciones publicadas [2], en los próximos cuatro años las ventas *on-line* crecerán entre un 10 % y un 15 % anual.

Sin embargo, todavía hay mucho trabajo que hacer en el campo del m-commerce. Uno de los aspectos que más negativamente afecta a su crecimiento es la falta de privacidad y confianza de los consumidores respecto a los comerciantes y a las transacciones *on-line*. Otro de los aspectos importantes, a menudo dejado de lado, es la baja eficiencia (medida como el tiempo de respuesta) de las soluciones de m-commerce percibida por los consumidores.

En el campo del m-commerce, los cupones electrónicos son uno de los temas que requiere importantes mejoras, sobre todo en privacidad, usabilidad y eficiencia. Un cupón electrónico es la versión electrónica de los cupones en papel, documentos impresos que permiten al consumidor conseguir o acceder a productos o servicios, normalmente bajo un descuento o beneficio. En este sentido, encontramos conocidas soluciones comerciales, como cupones para restaurantes [3], [4], hoteles [5], etc., aunque todas ellas se basan en la utilización final del papel para poder canjearlos en los comercios. Este modo de funcionamiento conlleva una pérdida en tiempo y recursos tanto para los comerciantes como para los consumidores y además frena su expansión.

Tanto los cupones electrónicos individuales como los multicupones (el equivalente a los talonarios de cupones) han atraído la atención en los últimos años de la comunidad científica [6]–[20]. No obstante, las soluciones no se validan teniendo en cuenta el tiempo total de respuesta percibido por los consumidores, a pesar que este es un aspecto crítico que debe ser considerado tanto en la fase de diseño como de implementación.

Contribución. En este artículo incidimos en la importancia de analizar todos los costes que influyen en el tiempo de respuesta de los protocolos. Para realizar este trabajo, hemos implementado en Java una solución propia de multicupones electrónicos para múltiples comerciantes [16], llamada $\mathcal{MC} - 2\mathcal{D}$ y hemos analizado su eficiencia y rendimiento. La eficiencia la medimos respecto a una propuesta previa similar de multicupones electrónicos, la cual fue verificada en un entorno limitado usando una sola computadora. Gracias a este análisis, demostramos que nuestra propuesta mejora ampliamente la solución previa. Finalmente, desplegando la implementación en un entorno de producción con dispositivos móviles Android, servidores remotos y comunicaciones reales, analizamos su rendimiento teniendo en cuenta los efectos de la red. Además de comprobar que $\mathcal{MC} - 2\mathcal{D}$ es viable en un entorno real, también demostramos que no solo la criptografía incide en aumentar el tiempo de respuesta percibido por los clientes del m-commerce, sino que otros costes pueden ser incluso mayores.

Organización. El artículo está organizado de la siguiente forma. En la Sección II presentamos un análisis sobre las propuestas previas. En la Sección III se resume la solución propuesta. La Sección IV se dedica a presentar una comparación de eficiencia basada en el número y tipo de operaciones criptográficas. Utilizando un escenario real, en la Sección V analizamos los diferentes factores que influyen en el rendimiento de la solución. Finalmente, cerramos el trabajo con las conclusiones y las líneas futuras en la Sección VI.

II. Trabajos Previos

Como se ha comentado en la introducción, existen propuestas tanto comerciales como de carácter científico para cupones electrónicos. Respecto a las soluciones comerciales [3]–[5],

ISBN: 978-84-9717-323-0

éstas intentar ofrecer soluciones sencillas a bajo coste y normalmente basadas en papel. Es decir, evitan en la medida de lo posible llevar a cabo nuevas inversiones en implementaciones y reutilizan los sistemas que ya tienen desarrollados. Por ejemplo, una manera sencilla que utilizan las compañías para ofrecer cupones electrónicos es desplegando una simple página web a través de la cual los clientes pueden comprar cupones para un determinado uso. Sin embargo, los clientes deben desplazarse físicamente hasta la tienda del comerciante (o a un establecimiento autorizado) o utilizar su propia impresora para obtener una copia en papel. Este modo de funcionamiento no facilita el uso de los cupones y limita su difusión.

Respecto a las propuestas científicas actuales referentes a cupones y multicupones electrónicos [6]–[20], éstas intentan ofrecer el mayor número de funcionalidades sin considerar el coste que pueden generar al aplicarse en escenarios reales. No obstante, solo un número reducido de ellas [13], [16] proponen soluciones para un entorno donde los usuarios puedan gastar sus cupones en diferentes comerciantes sin tener que emitir un multicupón para cada uno de ellos (escenarios multi-comerciante). Por otra parte, en muchas de las propuestas no se encuentra suficiente información para analizar su viabilidad, tanto la referente a la implementación de las operaciones criptográficas involucradas como a la eficiencia resultante. En la mayoría de los trabajos que proporcionan medidas de eficiencia, utilizan escenarios de laboratorio, con pruebas limitadas y sin tener en cuenta todos los factores que influyen en el rendimiento final de las soluciones. Los autores de [8], [10] analizan sus propuestas basándose en cómo el número de cupones contenidos en un multicupón incrementa el coste de los diferentes protocolos para su gestión. Como resultado, los autores en [8] afirman que el coste es lineal respecto al número de cupones involucrados en cada transacción, mientras que en [10] se afirma (sin aportar ninguna prueba) que su esquema tiene un coste computacional constante con independencia del número de cupones involucrados en cada transacción. En [21], el autor realiza una implementación del esquema presentado en [13], pero considerando un entorno de pruebas local, en donde todas las operaciones se ejecutan sobre una misma computadora. Otras propuestas de cupones electrónicos [6], [15], [17]–[19] proporcionan resultados de eficiencia en entornos muy limitados y en pocos casos consideran el uso de algún tipo de dispositivo móvil [20].

Por lo tanto, la evaluación de soluciones para multicupones se ha realizado principalmente en términos del número de operaciones criptográficas. Sin embargo, este tipo de análisis no puede asegurar la viabilidad de una propuesta sobre redes y dispositivos reales. Este es un aspecto crítico para el éxito del m-commerce en general y de las soluciones para multicupones electrónicos en particular.

III. Una Solución de Cupones Electrónicos

A continuación resumimos los puntos fundamentales de $\mathcal{MC}-2\mathcal{D}$, solución de multicupones electrónicos para escenarios multi-comerciante. Los detalles de la misma, así como un amplio análisis de seguridad se pueden consultar en [16].

III-A. ¿Cómo Proporcionar Privacidad?

El funcionamiento de la solución se basa en el uso de la firma parcial ciega y la firma de grupo.

Firma parcial ciega. Es una generalización de la firma ciega [22] en la que el firmante tiene la capacidad de añadir a la firma resultante un conjunto de datos comunes acordados previamente entre el firmante y el solicitante. $\mathcal{MC}-2\mathcal{D}$ usa el esquema de firma parcial ciega presentado en [23].

Firma de grupo. Es una primitiva criptográfica que genera firmas en las que la identidad de un firmante que pertenece a un grupo de usuarios se mantiene en secreto. En estos esquemas se define una tercera parte, llamada *Gestor de grupo*, que es el encargado de generar los parámetros necesarios para realizar estas firmas. Además, es la única entidad capaz de revocar el anonimato y revelar la identidad de la entidad firmante. En nuestra solución se usa el esquema de firma de grupo propuesto en [24].

III-B. Arquitectura y Protocolos

La Figura 1 representa la arquitectura de la solución $\mathcal{MC}-2\mathcal{D}$. Los participantes involucrados son el cliente ($\mathcal{C}$), el vendedor ($\mathcal{V}$), el emisor ($\mathcal{E}$) y el gestor de grupo ($\mathcal{G}$). Entre cada uno de los participantes se definen siete protocolos: `Inicialización`, `Afiliación/Desafiliación`, `Registro`, `Emisión`, `Pago Múltiple`, `Depósito` y `Reembolso`.

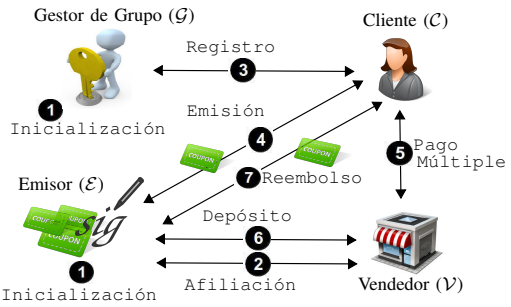

Figura 1: Arquitectura de $\mathcal{MC}-2\mathcal{D}$.

1. Inicialización. Tanto $\mathcal{G}$ como $\mathcal{E}$ inicializan sus servicios para recibir peticiones. $\mathcal{G}$ crea un conjunto de claves secretas y una clave pública para el esquema de firma de grupo, mientras que $\mathcal{E}$ y los clientes generan sus propias claves RSA.

2. Afiliación / Desafiliación. Todos los vendedores interesados en aceptar cupones emitidos por $\mathcal{E}$ se afilian a $\mathcal{E}$ mediante un simple acuerdo sin que se lleve a cabo ningún intercambio de información sensible.

3. Registro. Cada cliente interesado en usar cupones tiene que registrarse con $\mathcal{G}$ mediante el protocolo de `Registro` usando su identidad real, para así obtener una pareja de claves de grupo. Entonces $\mathcal{G}$ enlaza la identidad real de $\mathcal{C}$ con su correspondiente clave secreta para poder revocar el anonimato en caso de ser necesario.

4. Emisión. El protocolo permite a $\mathcal{C}$ solicitar a $\mathcal{E}$ la emisión de un multicupón firmado, al que llamamos $\mathbb{MC}^{2D}$.

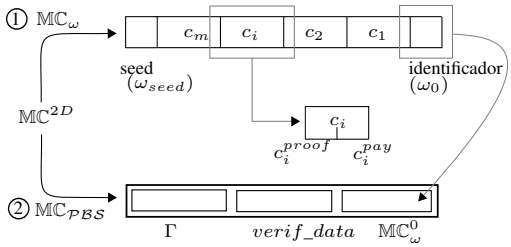

Figura 2: Estructura $\mathbb{MC}^{2D}$ compuesta por $\mathbb{MC}_\omega$ (considerando un sola tira de m cupones) y $\mathbb{MC}_{\mathcal{PBS}}$.

La estructura $\mathbb{MC}^{2D}$ (Figura 2) está compuesta por dos elementos principales: $\mathbb{MC}_\omega$ y $\mathbb{MC}_{\mathcal{PBS}}$.

1. $\mathbb{MC}_\omega$. Es la estructura que define todos los cupones que forman un multicupón. $\mathbb{MC}_\omega$ se organiza en múltiples tiras de cupones, cada una de ellas con un número determinado de cupones y con el mismo valor (o descuento). Para cada tira de m cupones, la solución genera iterativamente (mediante *hash chain*) $2m+1$ hashes desde un identificador aleatorio y secreto (*identificador seed*: ω_{seed}) hasta el último hash de la tira (*identificador de la tira*: ω_0). Entonces, cada cupón (c_i) se define mediante dos hashes: el de la derecha es la *información de pago* $(c_i^{pay} = \omega_{2i-1})$ y el de la izquierda es la *información de prueba* $\left(c_i^{proof} = \omega_{2i}\right)$, $\forall 0 < i \leq m$ (i indica el i-*ésimo* cupón de la tira). $\mathcal{C}$ mantiene $\mathbb{MC}_\omega$ en secreto, excepto el elemento ω_0, como veremos a continuación.
2. $\mathbb{MC}_{\mathcal{PBS}}$. Es la firma parcial ciega sobre $\mathbb{MC}_\omega^0$, la lista de todos los ω_0 contenidos en $\mathbb{MC}_\omega$. El elemento $\mathbb{MC}_{\mathcal{PBS}}$ contiene además datos de verificación $(verif\_data)$ así como información pública y acordada previamente (Γ) entre $\mathcal{C}$ y $\mathcal{E}$. Ésta define las características de $\mathbb{MC}^{2D}$: número de tiras y número de cupones en cada tira, el valor o descuento de cada cupón, marcas temporales para limitar su validez, etc.

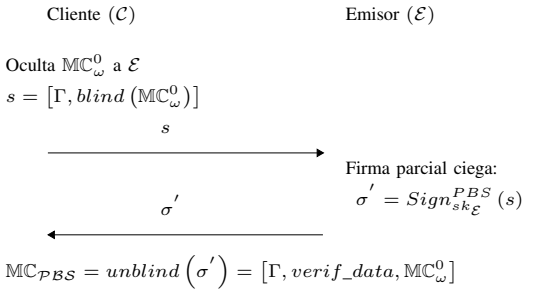

Figura 3: Protocolo de `Emisión`.

Una vez $\mathcal{C}$ ha generado $\mathbb{MC}_\omega$, empieza el protocolo de `Emisión` (Figura 3). La emisión de un multicupón implica la ejecución de un proceso basado en una firma parcial ciega sobre $\mathbb{MC}_\omega^0$, mediante el cual $\mathcal{E}$ firma $\mathbb{MC}_\omega^0$ (aunque no pueda obtener los datos en claro), juntamente con la información común (Γ). Como resultado, $\mathcal{C}$ obtiene $\mathbb{MC}_{\mathcal{PBS}}$, elemento que $\mathcal{E}$ no puede reconocer. Además, $\mathbb{MC}_{\mathcal{PBS}}$ no contiene ninguna información referente a la identidad de $\mathcal{C}$, gracias al uso de la firma parcial ciega.

5. `Pago Múltiple`. $\mathcal{C}$ puede pagar con cupones usando el protocolo de `Pago Múltiple` (Figura 4) a cualquiera de los $\mathcal{V}$ afiliados a $\mathcal{E}$. El protocolo de `Pago Múltiple` tiene cuatro pasos, mediante los cuales $\mathcal{C}$ puede gastar cualquier número de cupones con una sola ejecución del protocolo, incluso cupones pertenecientes a diferentes tiras de cupones. Esta característica no incluida en propuestas previas contribuye a mejorar la eficiencia de nuestra solución.

$\mathcal{C}$ firma usando el esquema de firma de grupo un conjunto de datos $(data_1)$ entre los cuales está la *información de pago* $(\mathbb{MC}_\omega^{pay})$. $\mathcal{V}$ valida la información y, si los datos recibidos son válidos ($\mathbb{MC}_\omega^{pay}$ no usado antes, $\mathbb{MC}_\omega^{pay}$ pertenece a $\mathbb{MC}_{\mathcal{PBS}}$, verificación de $\mathbb{MC}_{\mathcal{PBS}}$, etc.), envía un acuse de recibo juntamente con el servicio solicitado. A continuación, se repite el proceso, esta vez usando otro conjunto de datos $(data_2)$ análogo al anterior, pero conteniendo la *información de prueba* $\left(\mathbb{MC}_\omega^{proof}\right)$. Como antes, si las verificaciones son satisfactorias, $\mathcal{V}$ envía un acuse de recibo.

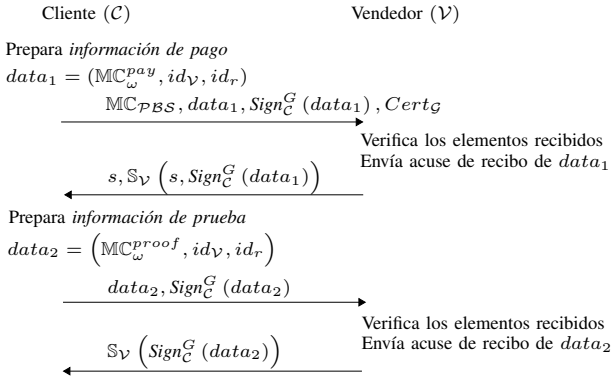

Figura 4: Protocolo de `Pago Múltiple`.

6. `Depósito` (*on-line* o *off-line*). El protocolo de `Depósito` permite a $\mathcal{V}$ solicitar a $\mathcal{E}$ un depósito correspondiente al valor de los cupones recibidos de los clientes. $\mathcal{V}$ puede depositar cupones por cada transacción de pago (`Depósito` *on-line*) o solo cuando tiene una lista de cupones (`Depósito` *off-line*).

7. `Reembolso`. En caso que $\mathcal{C}$ quiera recuperar el valor de cupones sin gastar, el protocolo le permite que $\mathcal{E}$ autorice su reembolso. Este protocolo es opcional y su aplicación dependerá de la implementación y del escenario.

IV. Comparación con una Propuesta Similar

A continuación comparamos la eficiencia de nuestra solución ($\mathcal{MC}-2\mathcal{D}$) frente al esquema multi-comerciante propuesto en [13]. Con el objetivo de comparar las medidas, hemos adaptado el escenario de pruebas a las condiciones de ejecución que los autores del esquema propuesto en [13] han realizado y analizado en [21] (un único portátil para cliente, comerciante y emisor, considerando la misma capacidad de cómputo). Además, hemos considerado las mismas pruebas

Cuadro I: Comparación práctica de rendimiento respecto a [13].

	Emisión (segundos)				**Pago Múltiple** (segundos)			
	$k = 5$ cupones			$k+1$	$k = 5$ cupones			$k+1$
	$\mathcal{C}$	$\mathcal{E}$	Total		$\mathcal{C}$	$\mathcal{V}$	Total	
[13]	-	-	4,280	0,811	-	-	33,01	6,476
Nuestra solución	0,023	1,182	1,205	$< 0{,}005$	0,877	1,204	2,082	$< 0{,}02$
Nuestra solución*	n/a	n/a	n/a	n/a	0,093	1,204	1,297	$< 0{,}02$

* - aplicando precomputación para la firma de grupo en el cliente durante el protocolo de `Pago Múltiple`
n/a - no aplicable

que en [21], teniendo en cuenta solo el tiempo de computación. De esta forma, comparamos el tiempo necesario para emitir y gastar un grupo de cinco cupones ($k = 5$) y la carga adicional de emitir o gastar un cupón adicional ($k + 1$). El Cuadro I recoge los resultados de rendimiento de ambas soluciones.

Analizando el proceso de emisión, el cliente solo necesita 23 *ms* de computación para obtener un $\mathbb{MC}^{2D}$, lo que significa que es aproximadamente 3,5 veces más rápido que el presentado en [21].

Referente al protocolo de `Pago Múltiple`, nuestra propuesta también obtiene mejores resultados. Tanto es así que el tiempo necesario para gastar 5 cupones es aproximadamente 15 veces menor que el mostrado en [21]. Si además aplicamos técnicas de precomputación para la firma de grupo, nuestro protocolo llegaría a ser hasta 25 veces más rápido, como se puede observar en el Cuadro I.

Finalmente, el tiempo necesario para emitir o gastar un cupón adicional en nuestro esquema, es despreciable. Esto es debido a que durante el protocolo de `Pago Múltiple`, $\mathcal{V}$ solo tiene que computar dos hashes para cada cupón adicional. Por tanto, aunque se gasten múltiples cupones durante una sola ejecución del protocolo, el tiempo de computación solo aumentará de forma lineal en función del coste de dos operaciones de hash por cada cupón. Como conclusión, el análisis demuestra que a diferencia de [13], $\mathcal{MC}-2\mathcal{D}$ es una solución escalable donde su rendimiento es independiente del número de cupones emitidos o gastados.

V. Evaluación del Rendimiento

Como hemos enfatizado en §I, no solo se debe tener en cuenta el coste computacional de las operaciones del protocolo, sino que también hay que introducir los costes debidos al efecto de la red. En esta Sección vamos a evaluar el rendimiento de $\mathcal{MC}-2\mathcal{D}$ utilizando un dispositivo Android como plataforma cliente. Además, hemos añadido la lógica necesaria para implementar la comunicación entre clientes y servidores remotos.

V-A. *Escenario de Pruebas*

La Figura 5 representa el escenario de pruebas considerado para obtener los valores de rendimiento de $\mathcal{MC}-2\mathcal{D}$. El escenario que proponemos emula un entorno real de producción con dispositivos móviles, servidores remotos y conexiones de red comerciales. Así pues, como plataforma de servidor, hemos elegido la solución Elastic Cloud Computing (EC2) de Amazon Web Services (AWS), para ejecutar el código

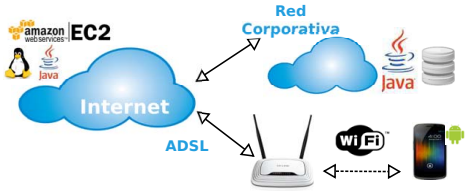

Figura 5: Escenario de pruebas.

del vendedor ($\mathcal{V}$), y un servidor virtual alojado en la red corporativa de la universidad, para ejecutar el código del emisor ($\mathcal{E}$). La aplicación cliente corre en un dispositivo Android, concretamente HTC Desire, que se conecta a los servidores remotos mediante una red WiFi y una conexión ADSL comercial. El Cuadro II resume las propiedades de los dispositivos considerados, mientras que el Cuadro III define las principales características de las dos redes consideradas.

Cuadro II: Dispositivos de test considerados.

Dispositivo	**Rol**	**CPU**	**RAM**	**OS**
Virtualbox	$\mathcal{E}$	2.8 GHz	1GiB	Debian Linux
EC2 μ-instance	$\mathcal{V}$	2 *EC2 CU*[(1)] ($\approx$ 1.0-1.2GHz)	633MiB	AWS Linux
HTC Desire	$\mathcal{C}$	1GHz	512MiB	Android 2.3

[(1)] Una *EC2 CU* (*Compute Unit*) proporciona la CPU equivalente a un procesador Xeon a 1.0-1.2GHz [25]

Cuadro III: Características de las redes.

Camino		**Tasa de transmisión (media)**		**Latencia (media)**
Origen	**Destino**	**Bajada**	**Subida**	**Round-trip**
$\mathcal{C}$ (ADSL)	$\mathcal{V}$	<3Mbps	<0.3Mbps	>200 ms
$\mathcal{V}$	$\mathcal{E}$	>25Mbps	>25Mbps	<100 ms

V-B. *Tiempo de Respuesta y Longitud de Mensajes*

Para conocer el rendimiento de la solución, hemos analizado el tiempo de respuesta total percibido por la aplicación cliente, realizando pruebas para los protocolos en las que está involucrada, es decir, los protocolos de `Registro`, `Emisión` y `Pago Múltiple`. Todas las pruebas se han repetido 20 veces y se ha realizado la media de los valores obtenidos descartando los resultados extremos.

En el tiempo de respuesta total percibido por el cliente, podemos distinguir dos factores principales:

- Tiempo de computación. La aplicación cliente tiene que realizar cálculos y operaciones matemáticas para generar las peticiones y procesar las respuestas recibidas. En este caso, los valores temporales dependen de la capacidad de procesamiento de cada dispositivo, principalmente de la CPU y de la memoria disponible.
- Tiempo de transmisión de red. El tiempo consumido por la aplicación para enviar y recibir datos a través de la red.

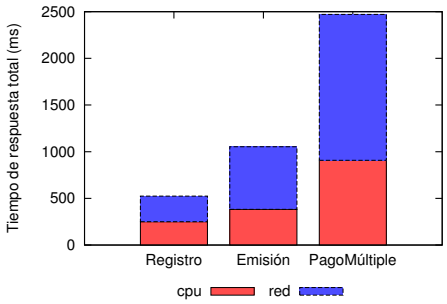

Figura 6: Tiempo de respuesta total para cada protocolo (usando HTC Desire y acceso WiFi).

La Figura 6 muestra el tiempo de respuesta medido en el cliente para cada uno de los protocolos analizados usando el dispositivo móvil HTC Desire. El protocolo que implica mayor coste es el de `Pago Múltiple`, dado que es el que incorpora mayor número de operaciones, tanto para cliente como para vendedor (entre las cuales hay que destacar dos firmas de grupo) y también un mayor tiempo de espera de red.

Si analizamos la Figura 7, podemos observar como la mayor parte del tiempo consumido por cada uno de los protocolos es básicamente debido a tareas de red: enviar mensajes y quedar en espera de recibir los mensajes de respuesta. Las tareas de red llegan a significar incluso más del 50 % del tiempo de respuesta total percibido por la aplicación cliente.

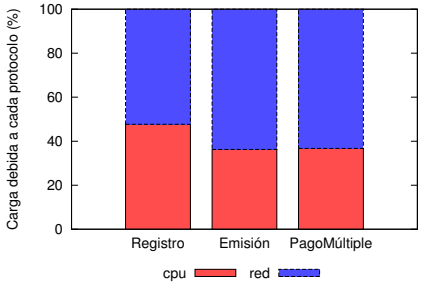

Figura 7: Porcentaje de carga debido a cada una de las tareas.

Si también analizamos el resultado obtenido teniendo en cuenta una ejecución *on-line* del protocolo de `Depósito` por parte del vendedor durante el `Pago Múltiple`, podemos afirmar que el tiempo añadido en el tiempo de total de respuesta es de solo 680 *ms*. Por consiguiente, el hecho de ejecutar una validación *on-line* de los cupones por cada ejecución del `Pago Múltiple`, representa un coste asumible en caso que se requiera comprobar inmediatamente con el emisor si los cupones recibidos no se han usado previamente.

En definitiva, además de evidenciar la eficiencia y el rendimiento de $\mathcal{MC}-2\mathcal{D}$, el análisis también demuestra que no solo es necesario evaluar el coste respecto al uso de los recursos de procesamiento necesarios, sino que también es imprescindible evaluar el tiempo consumido en la transferencia de datos a través de la red. Tanto es así que hemos demostrado que el tiempo necesario para enviar y recibir mensajes, puede ser incluso más importante que el tiempo de procesamiento de los mismos mensajes.

VI. Conclusiones

En este trabajo hemos comprobado como nuestra propuesta de cupones electrónicos para el escenario multi-comerciante es eficiente, escalable y que puede ser usada en dispositivos móviles. Para demostrarlo, hemos implementado la solución, comparado su eficiencia respecto a la propuesta previa y analizado su rendimiento considerando un escenario real. En primer lugar, la comparación nos permite afirmar que $\mathcal{MC}-2\mathcal{D}$ es más eficiente, utilizando el mismo escenario de pruebas que la propuesta anterior y considerando solo el efecto de la computación. Esto es debido, principalmente, a la utilización de mecanismos criptográficos con una menor carga y a la capacidad de nuestro esquema de permitir emitir y gastar cupones utilizando una misma transacción. En segundo término, la implementación completa del esquema sobre la plataforma Android nos ha permitido realizar una evaluación del rendimiento considerando un escenario realista, con servidores remotos y comunicaciones reales, escenario alejado de los entornos de prueba limitados que normalmente encontramos en las propuestas científicas. De esta manera, las medidas reflejan todos los factores que pueden afectar al tiempo de respuesta. De hecho, hemos podido comprobar que los costes debidos a otras tareas diferentes a la computación deben también ser analizados cuidadosamente para obtener una solución viable y con un tiempo de respuesta adecuado para el entorno de ejecución de la misma.

Como trabajo futuro, sería interesante estudiar la viabilidad de llevar a cabo el pago con cupones en los comercios utilizando tecnología NFC.

Agradecimientos

Este trabajo ha sido parcialmente financiado por el Ministerio de Educación y Ciencia bajo el proyecto CONSOLIDER-ARES (CSD2007-00004).

Referencias

[1] BuddeComm. Global Mobile Communications - Statistics, Trends and Regional Insights. Report, verificado en Abril, 2014. http://goo.gl/Vw40qu.

[2] Techcrunch. Forrester 2012-2017: e-Commerce Forecast Analysis. Sitio web, verificado en Abril, 2014. http://goo.gl/7Dtwup.

[3] Edenred. Compañía internacional de talonarios de cupones para restaurantes. Sitio web, verificado en Abril, 2014. http://www.edenred.com.

[4] Gourmet. Compañía internacional de talonarios de cupones para restaurantes. Sitio web, verificado en Abril, 2014. http://www.cheque-dejeuner.com/.

[5] Bancotel. Compañía internacional de talonarios de cupones para hoteles. Sitio web, verificado en Abril, 2014. http://www.bancotel.es/.

[6] Boying Zhang, Jin Teng, Xiaole Bai, Zhimin Yang, and Dong Xuan. P3-coupon: A probabilistic system for Prompt and Privacy-preserving electronic coupon distribution. In *PerCom*, pages 93–101. IEEE, 2011.

[7] Carlo Blundo, Stelvio Cimato, and Annalisa De Bonis. Secure e-coupons. *Electronic Commerce Research*, 5:117–139, January 2005.

[8] Liqun Chen, Matthias Enzmann, Ahmad-Reza Sadeghi, Markus Schneider, and Michael Steiner. A Privacy-Protecting Coupon System. In *Financial Cryptography and Data Security*, volume 3570 of *Lecture Notes in Computer Science*, pages 578–578. Springer-Verlag, Berlin, Heidelberg, 2005.

[9] Sébastien Canard, Aline Gouget, and Emeline Hufschmitt. A handy multi-coupon system. In *Applied Cryptography and Network Security*, volume 3989 of *Lecture Notes in Computer Science*, pages 66–81. Springer-Verlag, Berlin, Heidelberg, 2006.

[10] Lan Nguyen. Privacy-protecting coupon system revisited. In *Financial Cryptography and Data Security*, volume 4107 of *Lecture Notes in Computer Science*, pages 266–280. Springer-Verlag, Berlin, Heidelberg, 2006.

[11] Liqun Chen, B. Alberto N. Escalante, Hans Löhr, Mark Manulis, and Ahmad-Reza Sadeghi. A privacy-protecting multi-coupon scheme with stronger protection against splitting. In *Proceedings of the 11th International Conference on Financial Cryptography and 1st International Conference on Usable Security*, volume 4886 of *Lecture Notes in Computer Science*, pages 29–44. Springer-Verlag, Berlin, Heidelberg, 2007.

[12] Alberto N. Escalante, Hans Löhr, and Ahmad-Reza Sadeghi. A non-sequential unsplittable privacy-protecting multi-coupon scheme. In *GI Jahrestagung (2)*, pages 184–188, 2007.

[13] Frederik Armknecht, B. Alberto N. Escalante, Hans Löhr, Mark Manulis, and Ahmad-Reza Sadeghi. Secure multi-coupons for federated environments: privacy-preserving and customer-friendly. In *Proceedings of the 4th International Conference on Information Security Practice and Experience*, volume 4991 of *Lecture Notes in Computer Science*, pages 29–44. Springer-Verlag, Berlin, Heidelberg, 2008.

[14] Liu Xin and Qiu liang Xu. Practical compact multi-coupon systems. In *IEEE International Conference on Intelligent Computing and Intelligent Systems (ICIS)*, volume 3, pages 211 –216, 2009.

[15] Sue-Chen Hsueh and Jun-Ming Chen. Sharing secure m-coupons for peer-generated targeting via eWOM communications. *Electronic Commerce Research and Applications*, 9:283–293, July 2010.

[16] A. Pere Isern-Deya, M.F. Hinarejos, JL. Ferrer-Gomila, and M. Payeras-Capellà. A secure multicoupon solution for multi-merchant scenarios. In *IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, pages 655–663, 2011.

[17] Xiaoling Dai and John Grundy. NetPay: An off-line, decentralized micro-payment system for thin-client applications. *Electronic Commerce Research and Applications*, 6(1):91–101, 2007.

[18] Jen-Ho Yang and Chin-Chen Chang. A low computational-cost electronic payment scheme for mobile commerce with large-scale mobile users. *Wireless Personal Communication*, 63(1):83–99, March 2012.

[19] Wenmin Li, Qiaoyan Wen, Qi Su, and Zhengping Jin. An efficient and secure mobile payment protocol for restricted connectivity scenarios in vehicular ad hoc network. *Computer Communications*, 35(2):188 – 195, 2012.

[20] Francisco Borrego-Jaraba, Pilar Castro Garrido, Gonzalo Cerruela García, Irene Luque Ruiz, and Miguel Ángel Gómez-Nieto. A Ubiquitous NFC Solution for the Development of Tailored Marketing Strategies Based on Discount Vouchers and Loyalty Cards. *Sensors*, 13(5):6334–6354, 2013.

[21] Alberto N. Escalante. Privacy-protecting multi-coupon schemes with stronger protection against splitting. In *Master's Thesis. Department of Computer Science. Saarland University*. 2008.

[22] David Chaum. Blind Signatures for Untraceable Payments. *Advances in Cryptology Proceedings of Crypto 82*, pages 199–203, 1983.

[23] Hung-Yu Chien, Jinn-Ke Jan, and Yuh-Min Tseng. RSA-based Partially Blind Signature with Low Computation. *International Conference on Parallel and Distributed Systems ICPADS 2001*, pages 385–389, 2001.

[24] Dan Boneh, Xavier Boyen, and Hovav Shacham. Short Group Signatures. In *Advances in Cryptology – CRYPTO 2004*, volume 3152 of *Lecture Notes in Computer Science*, pages 227–242. Springer-Verlag, Berlin, Heidelberg, 2004.

[25] Amazon Web Services. Amazon Elastic Compute Cloud: Instance Types and Compute Resources Measurement, verificado en Abril, 2014. http://goo.gl/k0CJhn.