Seguridad en Entornos de Comunicaciones D2D Oportunistas Multioperador

Maitane Chaves(1), Patricia Ortiz(1), Ivan Prada(1), Oscar Lazaro(1), Baldomero Coll-Perales(2)
mchaves@innovalia.org, portiz@innovalia.org, iprada@innovalia.org , olazaro@innovalia.org, bcoll@umh.es
(1) Asociación Innovalia.
(2) Laboratorio Uwicore. Universidad Miguel Hernández de Elche

***Abstract*- Mobile operators are facing a major challenge trying to cope with the exponential growth of data traffic generation triggered by the boost of smartphones. With the aim of enabling the reduction of traffic load on operators' infrastructures, an architecture that exploits in a synergic way a diverse set of offloading D2D schemes has been proposed. However, this model, in spite of providing a significant reduction of traffic load, poses significant security challenges. This paper proposes a security solution whose objective is to guarantee the correct authentication and integrity of the Device-to-Device (D2D) communications in an efficient way, by making use of encryption techniques, users' anonymisation and trust and reputation, assuring data confidentiality and integrity, as well as end-to-end protection. Moreover, this paper presents the first simulation results regarding the performance evaluation of the key and pseudonyms distribution algorithms.**

I. INTRODUCCIÓN

El tráfico de datos móviles está creciendo exponencialmente con el uso generalizado de los Smartphones, y las comunicaciones M2M [1], lo cual plantea un reto importante en términos de capacidad para los operadores [2], cuyas infraestructuras no son capaces de soportar todo el tráfico adicional generado por los usuarios. Un enfoque posible para hacer frente a esta crisis de capacidad es mediante el incremento de la granularidad de las antenas desplegadas, es decir, mediante el despliegue de mayor número de antenas con menor cobertura, conocidas como Small Cells. Sin embargo, la necesidad de infraestructura "adicional" tiene costos significativos tanto en el despliegue como en las fases de planificación y gestión, requiriendo su escalado una planificación minuciosa. Por lo tanto, esta solución aisladamente no es capaz de satisfacer la creciente demanda de capacidad de datos a las que se enfrentan las redes actuales y futuras. Otras alternativas emergentes que actualmente se consideran como parte de la evolución 5G de la red incluye la migración del tráfico de datos móviles de la infraestructura del operador a los dispositivos (offloading) [3], aprovechando las capacidades de conexión de los actuales Smartphones para transmitir los datos mediante comunicaciones dispositivo a dispositivo (Device-To-Device - D2D) [4], y la integración de las comunicaciones celulares, Wi-Fi y ad-hoc o comunicaciones D2D, constituyendo las denominadas redes celulares multi-hop (Multi-Hop Cellular Netwoks - MCN) [5] [6].

El organismo de estandarización 3GPP está trabajando paralelamente en las comunicaciones D2D oportunistas. De hecho, el soporte a los Servicios de Proximidad (ProSe) y la estandarización D2D se ha convertido en una de las piezas claves de la versión 13 del estándar LTE y, por tanto, de las futuras redes celulares (4G y 5G).

En línea con esta última aproximación, en el proyecto MOTO [5] se propone una arquitectura para gestionar de manera eficiente el offloading de tráfico en entornos multi-operador. MOTO explota de forma sinérgica un conjunto de esquemas de offloading, incluyendo la descarga de LTE a otras infraestructuras inalámbricas (tales como Wi-Fi), así como el uso de comunicaciones ad-hoc multi-hop entre dispositivos de usuarios. Esta arquitectura, enfocada a resolver las necesidades de los entornos D2D oportunistas donde hay muchos operadores LTE y Wi-Fi, ofrece, además de la reducción de la carga en las infraestructuras de los operadores, la reducción de los retardos en las comunicaciones al posibilitar la transmisión de contenido entre usuarios en base a su proximidad.

Sin embargo, este tipo de esquemas de comunicaciones plantean importantes retos de seguridad, puesto que son susceptibles a numerosos ataques, que pueden poner en peligro no sólo la seguridad de las comunicaciones, sino también la privacidad de los usuarios y la integridad de la información transmitida. Es por ello que es necesario encontrar soluciones que sean capaces de garantizar la seguridad extremo a extremo y la privacidad de los usuarios, sin que su posición o identidad sea desvelada a usuarios malintencionados.

Este artículo presenta la propuesta de seguridad en redes de comunicaciones móviles oportunistas (D2D offloading) multi-operador. El modelo de seguridad propuesto está basado en la aplicación de técnicas criptográficas, el anonimato de los usuarios mediante el uso de pseudónimos de sesión y la creación de un marco de confianza, basado en la recolección de respuestas de usuario y gestión de confianza y reputación. Este artículo está organizado de la siguiente manera: la Sección II presenta distintos trabajos de investigación relacionados con la seguridad en entornos oportunistas, la Sección III describe la solución propuesta por el proyecto MOTO en la que se basa la propuesta de seguridad, así como los retos de seguridad que se presentan en este entorno y los objetivos que el modelo de seguridad debe de disponer. La Sección IV describe la solución propuesta y la Sección V los primeros resultados de simulación obtenidos. Finalmente, la Sección VI presenta las conclusiones alcanzadas.

II. TRABAJOS DE INVESTIGACIÓN RELACIONADOS

Cuando la confianza entre usuarios no se puede garantizar (es decir, cuando dispositivos maliciosos llevan a cabo únicamente acciones aparentemente legítimas), mitigar la acción de nodos maliciosos internos es un problema muy difícil de solucionar en redes oportunistas, y por lo general requiere transmitir gran cantidad de contenido redundante entre los

dispositivos. La movilidad sólo hace el problema más difícil: garantizar la integridad del mensaje multi-hop requiere un alto "umbral dinámico" o sólo da garantías probabilísticas. Se espera que las arquitecturas de seguridad móvil que sean eficientes en entornos oportunistas utilicen alguna aproximación en base a marcos de confianza.

Poonguzharselvi et al. [7] presenta un marco de confianza donde los nodos de la red siguen un modelo de movilidad basado en el traceo. La selección del siguiente salto se basa tanto en el valor de confianza, como en el movimiento del nodo hacia el destino.

Es importante tener en cuenta que la seguridad mediante el uso de marco de confianza, ha de protegerse ante ataques tipo Sybil, en los que un nodo malicioso suplanta y/o falsifica identidades. La prevención de ataques Sybil en redes oportunistas requiere una autenticación dedicada y un esquema de administración de claves. Shikfa [8] propone una gestión de claves que integra las asociaciones de seguridad con el descubrimiento de los nodos vecinos mediante el uso de certificados y firmas.

Otro aspecto importante a tener en cuenta es la privacidad, ya que los protocolos de enrutamiento oportunistas hacen uso de información que puede ser sensible a divulgaciones. Algunos protocolos abordan esta problemática restringiendo la redifusión a "grupos de confianza", en este sentido, el protocolo HiBOp [9] aplica el concepto de comunidad, al considerar que la exposición de información de contexto (durante el envío de mensajes) a nodos que pertenecen a una misma comunidad es aceptable, y asumiendo confianza entre todos los nodos de una misma comunidad. En consecuencia, los mensajes sólo pueden ser enviados a los nodos intermedios que provienen de la misma comunidad que los nodos de destino. Esta aproximación reduce considerablemente las posibilidades de revelación de información sensible en los protocolos de enrutamiento, pero no evita su divulgación ante nodos maliciosos.

III. Entorno Moto

El objetivo de MOTO es proporcionar una solución para descargar el tráfico de datos de las redes de operadores en favor de las capacidades de conectividad de los dispositivos de usuario. Para ello, se considera la existencia de una plataforma en la nube responsable de coordinar la difusión de contenido (plataforma MOTO) entre los usuarios que lo han solicitado. Este esquema de funcionamiento servirá para liberar a los operadores de la difusión de contenido redundante. La plataforma MOTO puede integrarse dentro o fuera de la red del operador. Cualquier aplicación de distribución de contenidos puede usar la plataforma para difundir contenido entre los usuarios del servicio. Este contenido será enviado por MOTO a ciertos usuarios "semilla" ("seed") que, a continuación, retransmitirán este contenido a través de conexiones multi-hop a otro usuarios, y estos a otros, hasta que la información llegue a los destinatarios finales (Figura 1).

De cara a poder proponer una solución de seguridad adecuada al contexto de difusión oportunista multi-operador propuesto en MOTO, es necesario analizar las características principales de las comunicaciones de un entorno como el propuesto: la topología es dinámica, los nodos pueden desplazarse durante la distribución del contenido los recursos limitados (vida de la batería y capacidades de procesamiento), los nodos pueden desconectarse en cualquier momento (perder la cobertura, desconectar las capacidades de conectividad, agotarse la batería, etc.) y los nodos pueden ser maliciosos o egoístas incluso una vez autenticados en la plataforma MOTO.

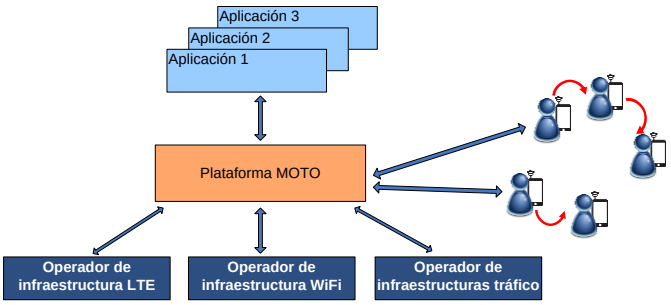

Fig. 1 Arquitectura MOTO

A. *Retos de seguridad en entornos oportunistas*

La naturaleza dinámica de las redes oportunistas plantea una serie de nuevos retos de seguridad y privacidad [10]. Por otra parte, el esquema de la comunicación que se establece en las redes oportunistas, como es el caso de MOTO, conlleva la necesidad de compartir la ubicación de los usuarios para gestionar la distribución de contenidos. Esto establece un nuevo desafío para la seguridad, dado que la privacidad de la ubicación se ha convertido en una de las preocupaciones principales en las redes móviles y hace particularmente difícil alcanzar un nivel satisfactorio de privacidad respecto a la ubicación en situaciones donde los nodos confían en los Servicios Basados en la Localización (LBS) [11].

Los principales riesgos que se presentan en el entorno MOTO en relación a los usuarios, son: (1) la posibilidad de inyectar contenido erróneo, es decir, que o bien el "seed" o el nodo que lo retransmite modifique el contenido antes de entregarlo; (2) que uno de los nodos no reenvíe el contenido y por lo tanto, los usuarios finales entren en la denominada "zona de pánico" y tengan que pedir el contenido a la plataforma MOTO de nuevo vía LTE y (3) la revelación de datos personales, es decir, que un nodo comunique a los otros nodos la identidad de un usuario de la plataforma o que un nodo intente monitorizar la actividad de otro usuario con el fin de obtener datos personales.

La solución de seguridad propuesta en este artículo debe evitar los riesgos citados anteriormente y, además, debe cumplir una serie de requisitos como son: confidencialidad, es decir, que los datos enviados no sean leídos por terceras partes, integridad de los datos, que consiste en poder detectar si los datos han sido modificados y, finalmente, disponibilidad de recursos, es decir, garantizar que los usuarios puedan acceder cuando lo necesiten.

IV. Solución de seguridad

La solución de seguridad que se propone en MOTO se basa en tres mecanismos principalmente: (1) criptografía, para proporcionar confidencialidad e integridad desde el origen de los mensajes, (2) anonimización de los usuarios mediante pseudónimos, para evitar divulgación de identidades y localización, y (3) gestión de la confianza y la reputación para identificar nodos maliciosos y egoístas. Con los mecanismos expuestos a continuación se pretende conseguir una seguridad extremo a extremo y garantías de privacidad tanto para el contenido como para los usuarios.

A. Criptografía

En primer lugar, como ya se ha comentado anteriormente en los objetivos de seguridad, es muy importante proporcionar confidencialidad, integridad y autenticidad de los datos transmitidos. Para cumplir estas expectativas se hace uso de técnicas de criptografía que se compone de tres niveles de seguridad.

El primer nivel está orientado a asegurar que el contenido a difundir a través de MOTO sólo sea "legible" por parte de los destinatarios que solicitan la información. El proveedor de contenidos debe cifrar el contenido que envía a través de los servicios de MOTO y distribuir la clave de dicha encriptación a los receptores finales externamente de manera segura (via LTE). De esta forma, se garantiza que sólo el destinatario final sea capaz de desencriptar el contenido para poder visualizar los datos enviados.

El segundo nivel tiene por objetivo proporcionar integridad de los datos y asegurar su origen. Este nivel se genera cuando la plataforma MOTO firma el contenido cifrado, que ha recibido del proveedor de contenidos, con su clave privada. Solamente los nodos pertenecientes a MOTO, que están en disposición de la clave pública de la plataforma MOTO, pueden hacerse con el contenido recibido del proveedor de contenidos. De esta forma, no será posible la modificación del contenido enviado sin que sea detectable por el destinatario de los datos.

Por último, el tercer nivel proporciona autenticación en las comunicaciones oportunistas, y garantiza que los nodos no acepten contenido de nodos no pertenecientes a los servicios MOTO. Este nivel comporta la encriptación que realiza cada nodo que retransmite el contenido (semilla o repetidor) con la clave pública de los nodos receptores (repetidor o destinatario). Con esta última capa de encriptación, se garantiza que sólo el nodo receptor sea capaz de desencriptar los datos con su clave privada.

B. Anonimización mediante pseudónimos

En segundo lugar, se pretende que ningún usuario a excepción de la plataforma MOTO pueda conocer la información personal del resto de usuarios: su identidad real, su localización a lo largo del tiempo o su actividad en la red. Esto se consigue sustituyendo el uso de datos personales de usuarios por el uso de un conjunto de pseudónimos junto con claves asimétricas, que cada usuario recibe de la plataforma MOTO. Los pseudónimos proporcionados están correlacionados con un usuario concreto y con pares de claves público-privadas en cada instante, y esta correlación únicamente es conocida por el usuario concreto que tiene asignado cada conjunto de seudónimos y claves, y por la plataforma MOTO, siendo inviable obtener dicha información por parte de otro usuario. En ningún momento se difunde entre los nodos la identidad real de un usuario, y para mayor confidencialidad, se estipula un intervalo de tiempo en el que los pseudónimos y las claves público-privadas se cambian para cada usuario. En el caso de desear mayor privacidad, se plantea la asignación de un mismo pseudónimo a distintos usuarios a lo largo del tiempo, evitando que se pueda seguir a un usuario en concreto a través del mismo.

Los nodos sólo intercambian los pseudónimos. Por lo tanto, si dos nodos quieren comunicarse y necesitan obtener la clave pública del otro, intercambian sus respectivos pseudónimos y con esos pseudónimos solicitan a la plataforma MOTO la clave pública del nodo con el que se van a comunicar. El hecho de que sea MOTO quien proporciona la clave pública garantiza que ésta se envía por una conexión segura (SSL/TLS) entre MOTO y el nodo además de que si el nodo es malicioso, es decir, su pseudónimo no es válido, éste no reciba la clave pública solicitada.

De esta forma, además de garantizar el anonimato, los usuarios no tienen que enviar sus claves por la red sino que es MOTO quien las proporciona de forma segura.

C. Gestión de la confianza y la reputación

En último lugar, se pretende garantizar un proceso de difusión óptimo entre los nodos de la red móvil oportunista, mediante un marco que gestiona la confianza y reputación de los usuarios de los servicios MOTO. La gestión de la confianza en una red ad-hoc usualmente se basa en el intercambio entre los nodos de información acerca de la misma (feedback) y en base a la información que cada nodo recopila sobre los demás, deciden si aceptan o no una conexión con un determinado nodo.

En el esquema de comunicaciones propuesto en MOTO, esto tiene un grado añadido de dificultad, puesto que la plataforma MOTO realiza la gestión del feedback pero no toma parte en las comunicaciones entre los nodos. Por lo tanto, tras la comunicación entre dos nodos en la red oportunista, estos envían un mensaje (feedback) a MOTO, que debe actualizar el nivel de confianza del nodo emisor. Ambos nodos envían un mensaje de feedback a MOTO, el emisor con la confianza que espera recibir, y el receptor con la que otorga al emisor. Este mensaje tiene una doble función, informar a la plataforma acerca de la recepción del contenido para tomar decisiones de difusión, y, monitorizar el comportamiento que tienen los nodos por motivos de seguridad.

El feedback cumple varios objetivos, (i) demostrar que el contenido recibido es correcto, mediante el envío del resultado de aplicar una función hash al contenido recibido (calculado en base al contenido encriptado por el proveedor de contenidos, es decir, a los datos del primer nivel de criptografía), (ii) que la comunicación efectivamente tuvo lugar mediante el envío del tiempo en el que se recibió el mismo, la identificación mediante pseudónimos del otro nodo involucrado y el rol del nodo que envía el feedback: emisor o receptor y (iii) la calidad de la conexión, basada en una escala definida previamente.

D. Distribución de claves

Para aplicar estos procedimientos de seguridad es necesario que los nodos obtengan las claves de una forma segura. En MOTO se plantea que el proveedor de contenidos sea el encargado de acordar la clave de sesión con el usuario final. A su vez, la plataforma MOTO es la encargada de distribuir las claves público-privadas a los nodos por el canal de control de la interfaz LTE por una comunicación segura (SSL/TLS).

V. Resultados de las Simulaciones

En esta sección se muestran los primeros resultados obtenidos a partir de las simulaciones que se están llevando a cabo de cara a comprobar la eficiencia de la solución propuesta. En concreto, hasta el momento se ha comprobado que la distribución de claves y pseudónimos propuesta no supone un tiempo sin servicio demasiado grande. Para realizar el análisis de la distribución de claves se han realizado simulaciones de Montecarlo. Se ha empleado un simulador de redes (ns-3) que proporciona modelos de cómo trabajan las

redes de paquetes de datos. Se ha configurado un escenario con los nodos de los usuarios así como con un nodo representando a la plataforma MOTO que se encarga del envío y recepción de las claves asimétricas y los pseudónimos. Las simulaciones se han enfocado en medir el tiempo que tarda la red en estabilizarse, es decir, el tiempo que pasa desde que se envía la primera clave hasta que todos los nodos de la red han recibido las nuevas claves y pseudónimos. En la simulación realizada, los nodos se sitúan y mueven aleatoriamente en toda el área de cobertura. La Tabla 1 resume los parámetros configurados en el escenario para las diferentes simulaciones. Se han realizado pruebas con dos longitudes de paquete distintas, con el fin de conocer si es viable enviar varios pares de claves y pseudónimos para tener que realizar la operación de refresco de claves con menos frecuencia y por consiguiente tener menos tiempo la aplicación sin servicio.

Parámetro	Valor
Número de eNBs	1
Número de nodos	10, 15, 50, 150
Longitud de las claves y pseudónimos	320 bits, 600 bits
Tiempo de vida de los mensajes	3 s
Tiempo del primer envío de tráfico	250 ms

Tabla 1.- Parámetros del simulador

En la Tabla 2, se muestran los resultados obtenidos en las diferentes simulaciones (95% intervalo de confianza). Como se puede observar el tiempo de estabilización (t_e) de la red en el peor de los casos es menor a 150 ms, lo que significa que el tiempo que la plataforma MOTO deja de dar servicio por esta causa es aceptable. Además, como se puede observar en las Figura 2, aunque el tiempo de estabilización de la red crece exponencialmente al aumentar el número de nodos, la diferencia entre enviar un paquete más pequeño y uno casi el doble de grande apenas incrementa el retardo.

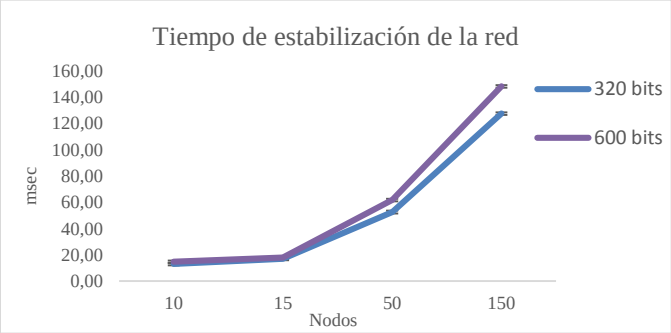

Fig 2.- Tiempo de estabilización de la red

Nodos	t_e; claves 320 bits	t_e; claves 600 bits
10	12,99 ms	14,68 ms
15	16,86 ms	17,88 ms
50	52,50 ms	61,73 ms
150	127,52 ms	148,17 ms

Tabla 2.- Tiempo de estabilización

VI. Conclusiones

En este trabajo se ha presentado una solución de seguridad eficiente para las redes D2D en entornos móviles donde, mediante las primeras simulaciones, se ha evaluado la eficiencia de los mecanismos de distribución-refresco periódico de las claves y pseudónimos para poder dotar a la red de la seguridad necesaria. Los resultados muestran un incremento exponencial en el tiempo de estabilización de la red con un número creciente de nodos. No obstante, los tiempos de estabilización de la red D2D (cuando todos los nodos están en posesión de las nueva credenciales) frente a los periodos de refresco, es decir, duración de sesión de servicios, indican que su aplicación para este tipo de despliegues es adecuada y con un impacto insignificante en el rendimiento del sistema.

Agradecimientos

Este trabajo ha sido financiado por el Ministerio de Economía y Competitividad y los fondos FEDER (TEC2014-57146-R). Está también parcialmente soportado por la Comisión Europea en el Proyecto del VII programa Marco MOTO (Mobile Opportunistic Traffic Offloading) bajo el contrato nº 317959.

Referencias

[1] R. Baldemai, «Evolving Wireless Communications: Addressing the Challenges and Expectations of the Future,» *IEEE Vehicular Technology Magazine*, vol. 8, nº 1, Marzo 2013.

[2] F. Rebecchi, M. Dias de Amorim, and V. Conan, «DROiD: Adapting to Individual Mobility Pays Off in Mobile Data Offloading,» *IFIP/IEEE Networking, Trondheim, Norway, June 2014.*

[3] Filippo Rebecchi, Marcelo Dias De Amorim, Vania Conan, Andrea Passarella, Raffaele Bruno, et al.., «Data Offloading Techniques in Cellular Networks: A Survey.,» *Communications Surveys and Tutorials, IEEE Communications Society, Institute of Electrical and Electronics Engineers (IEEE)*, pp. 1-25, 2014.

[4] M.J. Yang, S.Y. Lim, H.J. Park, and N.H. Park, «Solving the data overload: Device-to-device bearer control architecture for cellulardata offloading,» *IEEE Vehicular Technology Magazine*, vol. 8, nº 1, pp. 31-39, Marzo 2013.

[5] B. Coll-Perales, J. Gozalvez, O. Lazaro y M. Sepulcre, «Opportunistic Multi-Hop Cellular Networking for Energy-Efficient Provision of Mobile Delay Tolerant Services,» *IEEE Vehicular Technology Magazine*, 2015.

[6] J. Gozalvez y B. Coll-Perales, «Experimental Evaluation of Multihop Cellular Networks Using Mobile Relays,» *IEEE Communications Magazine*, vol. 51, nº 7, pp. 122-129, 2013.

[7] «MOTO,» [En línea]. Available: http://www.fp7-moto.eu/.

[8] B.Poonguzharselvi, V.Vetriselvi, «Trust framework for data forwarding in Opportunistic networks using mobile traces,» *International Journal of Wireless & Mobile Networks (IJWMN)* , vol. 4, nº 6, December 2012.

[9] Shikfa A, Onen M & Molva R, «Bootstrapping security associations in opportunistic networks,» *Proceedings of the 8th IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops)*, pp. 147-152, 2010.

[10] C. Boldrini, M. Conti, A. Passarella,, « Exploiting users' social relations to forward data in opportunistic networks: the HiBOp solution,» *Elsevier Pervasive and Mobile Computing*, vol. 4, nº 5, pp. 633-657, October 2008.

[11] Adrian Leung, Chris Mitchell, Royal Holloway, «A service discovery threat model for ad hoc networks,» de *University of London. Proceedings of the International Conference on Security and Cryptography (SECRYPT 2006)*, Setubal, 2006.

[12] S. Z. a. M. Radenkovic, «Utilizing Social Links for Location Privacy in Opportunistic Delay-Tolerant Networks,» *IEEE International Conference School of Computer Science, University of Nottingham, published in Communications (ICC)*, 2012.