Autenticación No Interactiva para Internet de las Cosas

Francisco Martín-Fernández, Pino Caballero-Gil, Cándido Caballero-Gil
Departamento de Ingeniería Informática
Universidad de La Laguna
Emails: francisco.martin.07@ull.edu.es, pcaballe@ull.es, ccabgil@ull.es

***Resumen*—En este trabajo se propone un esquema de intercambio de información confidencial en entornos no seguros sobre redes móviles ad-hoc, basado en el concepto de demostración de conocimiento nulo no interactiva. De esta manera, se consigue que en una única comunicación se puedan inferir datos relevantes para la verificación de la legitimidad de los nodos de la red. Además, se propone el uso de este esquema aplicado a la autenticación y el control de accesos, a través del establecimiento de claves mediante la idea del protocolo criptográfico de Diffie-Hellman.**

***Palabras clave*—Autenticación (*Authentication*), Privacidad (*Privacy*), Demostración de Conocimiento Nulo (*Zero Knowledge Proof*), Internet de las Cosas (*Internet of Things*)**

I. Introducción

Cada vez es más frecuente ver cómo la tecnología se funde con la realidad en el uso cotidiano. A esta tendencia se le conoce como la Internet de las Cosas o IoT (Internet of Things) y surge ante la necesidad de tener monitorizado e interconectado cualquier dispositivo electrónico que sea útil para el ser humano. En esta nueva dimensión aparecen nuevos retos relacionados con la seguridad inalámbrica, ya que esta es la vía convencional de comunicación entre estos objetos hiperconectados. Se necesitan algoritmos criptográficos ligeros acordes a la capacidad reducida de cómputo de estos dispositivos. Gracias a la aparición de tecnología cada vez más potente y reducida en tamaño y peso, los esquemas criptográficos en comunicaciones inalámbricas han ido cambiando a pasos agigantados para adaptarse a esas nuevas condiciones. En particular, la evolución de las redes hacia la IoT ha conllevado que este proceso se acelere.

Con la aparición de este nuevo paradigma de objetos interconectados, donde la dimensión física se mimetiza con la dimensión lógica, será necesario codificar más de 100.000 millones de objetos, lo que equivaldría a que cada ser humano esté rodeado por 3000 objetos de media. Un aspecto fundamental a tener en cuenta es la forma de comunicación entre estos objetos. Debido al carácter móvil y al reducido tamaño de muchos de estos artilugios que conforman la Internet de las Cosas, esta comunicación debe ser inalámbrica. Además, la forma de agrupación a la que tienden según su naturaleza desemboca en que ese tipo de comunicación inalámbrica se establezca mediantes las denominadas redes móviles ad-hoc, también conocidas como MANETs (Mobile Ad-hoc NETworks). Estas redes están compuestas por dispositivos móviles, conectados inalámbricamente y generalmente se caracterizan por poseer algunas propiedades de auto-configuración.

Cada dispositivo que forma parte de una MANET posee libertad para desplazarse, lo que implica que las condiciones de enlace entre los dispositivos cambian dinámicamente y que cada nodo actúa como router de las comunicaciones ajenas. Otro aspecto relevante de la tipología de esta red es que en general puede operar de forma autónoma o bien estar conectada a Internet. Esta última posibilidad es muy útil en aquellas situaciones en las que los propios dispositivos no tengan una conexión directa a Internet.

En las MANETs existen muchos tipos de amenazas que podrían llegar a condicionar su uso. Una de las mayores amenazas es contra la seguridad de las comunicaciones mediante ataques de suplantación de identidad o escucha de la información enviada entre los nodos de la red.

Este trabajo propone el diseño de un nuevo esquema criptográfico ligero, en concordancia con la capacidad de cómputo de los nodos de la red, que permita asegurar las comunicaciones inalámbricas en una MANET.

Este trabajo se estructura en varias secciones. En la sección II se introducen brevemente algunos antecedentes. La sección III trata de forma pormenorizada un nuevo esquema de autenticación no interactiva. En la sección IV se explican posibles casos de uso alternativo para el esquema propuesto. Por último, en la sección V se detallan algunas conclusiones.

II. Antecedentes

En la bibliografía existen muchas propuestas [6], tanto basadas en criptografía simétrica [15] como en criptografía asimétrica [16]. La seguridad de muchos de los primeros esquemas es bastante fuerte, pero su mayor inconveniente es la distribución de la clave común entre los participantes en la comunicación. En un entorno como el de las MANETs [4] aplicadas a la Internet de las Cosas [1], presuponer la existencia de un canal totalmente seguro para transmitir claves simétricas sería una utopía. Además, el número de claves que se necesitaría sería demasiado elevado en una gran MANET basada sólo en criptografía simétrica. Precisamente para intentar subsanar este problema nació la criptografía asimétrica, también conocida como criptografía de clave pública. Además, la criptografía de clave pública permite firmar digitalmente la comunicación si primero el emisor cifra con su clave privada y luego el receptor descifra con la clave pública del emisor,

ISBN: 978-84-9717-323-0

ya que así se consigue a la vez la identificación del remitente y la autenticación del mensaje. Curiosamente la capacidad de firma digital que otorga la criptografía de clave pública es lo que permite resolver el principal reto que presenta, que es la necesidad de establecer confianza en las claves públicas usadas. Para impedir posibles ataques MitM (Man in the Middle), se debe asegurar la identificación del usuario a quien corresponde cada clave pública. Existen diversos modelos para lograr esta certificación de claves públicas. El más habitual se basa en una infraestructura de clave pública o PKI (Public Key Infrastructure), que se basa en autoridades certificadoras. Otros esquemas se basan en una web de confianza. Una alternativa a las PKI es el uso de la criptografía basada en identidad en la que se hacen innecesarios los certificados.

El mayor inconveniente de los esquemas de criptografía asimétrica es su eficiencia computacional ya que en general los cálculos necesarios requieren bastante tiempo. Son sistemas, por lo general, demasiado pesados como para que funcionen con fluidez en entornos ligeros, como el de las MANETs en la IoT. Para subsanar este inconveniente se propone aquí la combinación de criptografía simétrica y de criptografía asimétrica mediante el uso de claves de sesión [5]. En particular, el modelo propuesto se basa en la generación de una clave de sesión compartida entre nodos previamente autenticados, con objeto de utilizar dicha clave de sesión para establecer comunicaciones secretas usando un sistema de criptografía simétrica.

Previo al establecimiento de las claves de sesión compartida se realiza una fase de autenticación de usuarios mediante un protocolo basado en la idea de las demostraciones de conocimiento nulo. Las demostraciones de conocimiento nulo o ZKP (Zero-Knowledge Proof) [10] establecen un método para probar el conocimiento de un secreto sin revelar ninguna pista sobre él.

En el ámbito de las MANETs usadas en IoT, una demostración de conocimiento nulo típica basada en sucesivos retos y respuestas implicaría un intercambio de sucesivos mensajes, lo que conllevaría tener que presuponer una conexión estable y continua entre los nodos. En entornos tan volátiles como la Internet de las Cosas, donde existen dispositivos que se pueden mover a gran velocidad (como por ejemplo, los vehículos que conforman las denominadas redes ad-hoc vehiculares o VANETs (Vehicular Ad-hoc NETworks), un intercambio masivo de mensajes para ejecutar una demostración de conocimiento nulo puede ser inviable debido a los posibles fallos de conexión durante el protocolo. Para subsanar el problema de la multitud de mensajes bidireccionales que producen las ZKP tradicionales han surgido en la bibliografía las demostraciones de conocimiento nula no interactivas [14], que condensan todos los retos en un único paquete enviado en un único mensaje. De esta forma el tiempo que conllevaría el intercambio de mensajes para llevar a cabo el protocolo interactivo se minimiza, de forma que sólo es necesario el envío de un único mensaje, pudiéndose incluso enviar este mensaje como beacon en modo broadcast a la red en la que se utilice el esquema.

III. Autenticación No Interactiva

Uno de los factores más importantes de los esquemas de demostración de conocimiento nulo, tanto interactivos como no interactivos, es la elección del problema matemático de base. En este trabajo en particular se utiliza el del isomorfismo de grafos. Un isomorfismo entre dos grafos se define mediante una biyección entre los conjuntos de sus vértices preservando la relación de adyacencia, o dicho de otro modo, cualquier par de vértices de un grafo son adyacentes si y solo si lo son sus imágenes en el otro grafo. El problema del isomorfismo de grafos consiste en determinar si dos grafos son isomorfos o no. Este problema ha sido utilizado en entornos criptográficos [12] [13] debido a que no se conoce un algoritmo eficiente para resolverlo en general. En particular, la determinación de si dos grafos con el mismo número de vértices v y de aristas a son isomorfos implicaría un ataque por fuerza bruta que exigiría comprobar si las $v!$ biyecciones posibles preservan la adyacencia. Curiosamente el problema del isomorfismo de grafos pertenece, en complejidad computacional, a la categoría NP, sin que se conozca hasta ahora si es resoluble en tiempo polinómico o bien si es NP-completo [11]. Por tanto su resolución, dependiendo del tamaño de los grafos implicados, puede ser muy costosa. Este problema permite crear varios compromisos a partir de un grafo original mediante sus posibles grafos isomorfos.

El esquema propuesto se basa en una variante de las demostraciones de conocimiento nulas no interactivas en la que sólo es necesario un único mensaje para poder verificar el conocimiento. La idea es conformar un sistema cuya seguridad pueda adaptarse según el nivel de seguridad que se requiera. De esta manera, cuanto más retos diferentes se consideren en la ejecución, más garantía tendrá el verificador. Concretamente los parámetros de la propuesta son:

- G: Grafo conocido por los nodos legítimos, sobre el que conocen una solución a un problema difícil.
- Sol_G: Solución al problema en G.
- $Reto_i$: Reto $i-$ésimo propuesto por el verificador.
- G_i: Grafo isomorfo $i-$ésimo usado como compromiso.
- $Iso(G, G_i)$: Isomorfismo entre G y G_i.
- $Res(Reto_i, G_i)$: Respuesta $i-$ésima correspondiente al $Reto_i$ sobre el grafo G_i.
- $h(\cdot)$: Función hash.
- $LSB(\cdot)$: Least Significant Bit o bit menos significativo de un string de entrada.
- $E_{k_i}(\cdot)$ Cifrado simétrico con clave k_i.
- $Subclave$: Contribución de un nodo a la clave de sesión.

Según la propuesta, el mensaje que cada nodo que desee autenticarse envía como nodo legítimo de la red está compuesto por una serie compromisos definidos mediante grafos isomorfos de un grafo conocido por todos los usuarios legítimos de la red. Por ejemplo, el grafo podría corresponderse con un grafo en el que los nodos representen a todos los usuarios de la red. En particular, esos compromisos se encuentran, todos salvo el primero, en principio cifrados de forma que se van descifrando a medida que se van verificando las respuestas anteriores.

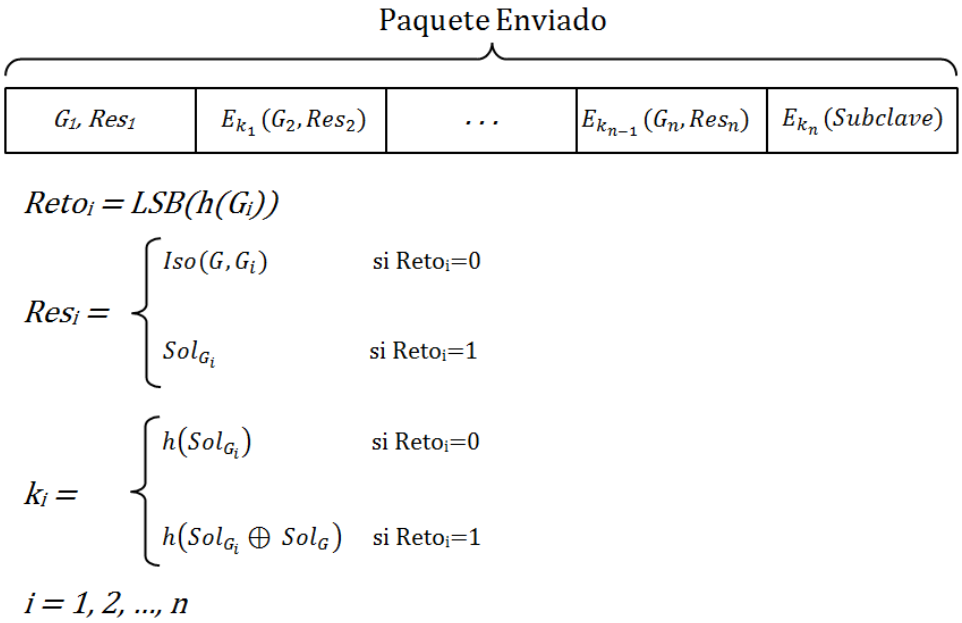

Figura 1. Componentes de los mensajes enviados según el esquema propuesto.

Concretamente el mensaje está dividido en segmentos cifrados con diferentes claves, exceptuando el primer segmento que está en claro (ver Figura 1). De esta manera, un usuario legítimo de la red puede autenticarse para unirse a una sesión si el verificador es capaz de descifrar todos los segmentos del mensaje y llegar a la parte de la contribución del otro nodo a la clave de sesión que se quiere compartir, que se esconde en el último segmento. Las claves de cifrado de cada segmento dependen del segmento anterior, de manera que aunque se pretenda descifrar únicamente el último segmento, es imposible ya que para ello se deben haber descifrado en cascada todos los segmentos anteriores. El nivel de seguridad del esquema depende del número de segmentos o retos que se incluyan en el mensaje ya que a mayor cantidad de segmentos, más complejo es llegar al último y obtener la información que se requiere para el establecimiento de la clave compartida. Tras la autenticación bidireccional siguiendo el mismo procedimiento, ambos nodos conocerán mediante un esquema del tipo Diffie-Hellman la clave de sesión compartida a partir de las dos subclaves intercambiadas.

Cada segmento contiene un grafo isomorfo del grafo original que conocen todos los usuarios legítimos del sistema. Además se establece una función hash unidireccional pública conocida por todos los nodos legítimos de la red. Por una parte esta función sirve para definir el reto que el usuario debe solucionar sobre cada grafo isomorfo de manera que sea conocido y estrictamente no maleable. Por otra parte, la función hash se utiliza en la definición de la clave de cifrado de cada segmento del mensaje.

El procedimiento de actuación del receptor del mensaje es:

1. Procesa el primer segmento del mensaje que está en claro.
2. Calcula, con la función hash, el reto que corresponde a la información que alberga el segmento.
3. Verifica si la respuesta corresponde al reto y grafo isomorfo.
4. A partir del reto calcula la clave que debe utilizar para descifrar el siguiente segmento.
5. Aplica los pasos del 2 al 4 hasta el último segmento, que una vez descifrado contiene la información necesaria para establecer la clave secreta compartida con el emisor.

Todos los usuarios legítimos de la red (ver Figura 2) poseen tanto el grafo original como una clave secreta correspondiente a dicho grafo, que es una solución a un problema difícil en ese grafo. Este podría ser por ejemplo un circuito hamiltoniano, ya que el problema del circuito hamiltoniano en un grafo arbitrario es NP-completo.

Como función hash, para discernir el reto correspondiente y calcular la clave de cifrado de cada segmento del mensaje se puede usar el nuevo estándar de función hash SHA-3 [2] [3].

En cuanto al cifrado simétrico para los distintos segmentos del mensaje, exceptuando el primero que se manda en claro, se puede optar por aplicar el cifrado en flujo usado en la cuarta generación de comunicaciones móviles (LTE o 4G) [8] [9], conocido como Snow3G [7], ya que entre sus características destaca una complejidad computacional lineal lo que garantiza eficiencia y rapidez en los procesos de cifrado y descifrado.

Como retos se han elegido los habituales aplicados a las demostraciones de conocimiento nulo basadas en grafos isomorfos. En el caso del esquema no interactivo planteado se definen los retos mediante el resultado de la función hash booleana aplicada sobre el grafo isomorfo compromiso. Para cada uno de los retos, la respuesta se define como sigue:

- $Reto = 0$: La respuesta es el isomorfismo.
- $Reto = 1$: La respuesta es la solución al problema en el

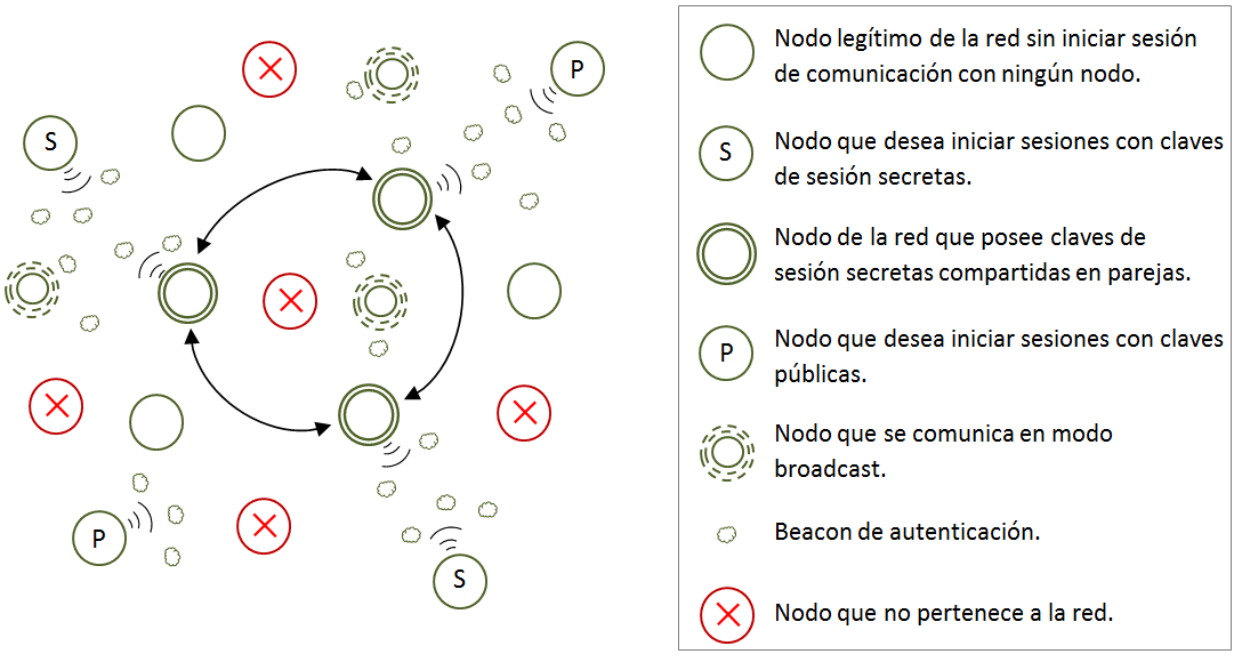

Figura 2. Tipos de nodos en el sistema propuesto.

grafo isomorfo.

A continuación se muestra el pseudocódigo de un posible algoritmo que debe ejecutar el receptor para implementar el esquema propuesto. Además en la figura 3 se muestra el diagrama de flujo de dicho algoritmo.

//Params: beacon, mensaje con segmentos cifrados
//Params: tseg, dimensión de los segmentos del beacon
//Params: solsec, solución al problema sobre el grafo G
//Return: Subclave, contribución a la clave obtenida del mensaje
function getDatos (char[] $beacon$, int tseg, char[] $solsec$)
01: var $segs$[]; // Almacena los segmentos del mensaje
02: // Se divide el mensaje en segmentos de tamaño $tseg$
03: $segs$ = $beacon$.splitByTam($tseg$);
04: // Se obtiene el grafo isomorfo y la respuesta en él
05: // Primer segmento que no está cifrado
06: var gi = getGi($segs$[0]);
07: var res = getRes($segs$[0]);
08: // Se calcula el reto a resolver
09: var $reto$ = LSB.hash(gi.getBytes());
10: // Comprueba que la respuesta es correcta para avanzar
11: **if** (res != respuesta(gi, $reto$))
12: return; // Si no es correcta se aborta
13: **endif**
14: // Obtiene la solución en gi
15: var sol = resolver(gi);
16: // ki es la clave de cifrado del segmento posterior
17: var $ki = \overline{reto} * hash(sol) \oplus reto * hash(sol \oplus solsec)$
18: var $descifrado$;
19: // Se repiten los siguientes pasos hasta el final
20: **for** (int $i = 1; i < segs.size() - 1; i++$){
21: // Se descifra el segmento con la clave ki
22: descifrado = Crypto.decrypt($segs[i]$, ki);
23: gi = getGi($descifrado$);
24: res = getRes($descifrado$);
25: $reto$ = LSB.hash(gi.getBytes());
26: **if** (res != respuesta(gi, $reto$))
27: return;
28: **endif**
29: sol = resolver(gi);
30: $ki = \overline{reto} * hash(sol) \oplus reto * hash(sol \oplus solsec)$
31: }
32: // El descifrado del último segmento sería
33: // la contribución a la clave compartida
34: return Crypto.decrypt($segs[segs.size()]$, ki);
endfunction

Una vez ejecutado el algoritmo descrito, sólo queda acceder al último segmento del mensaje y descifrarlo con la clave devuelta en la última iteración para poder obtener la contribución del nodo emisor a la clave de sesión compartida con cada uno de sus posibles interlocutores.

IV. Casos de Uso

Los principales casos de usos del esquema descrito son todos aquellos en los que se requiera el nivel de confidencialidad que otorgan las comunicaciones cifradas con claves de sesión secretas. De este modo, un caso de aplicación interesante podría ser el de las transacciones comerciales en MANETs. En este escenario, un nodo legítimo de la red quiere compartir un recurso propio con otros nodos legítimos para llevar a cabo una transacción comercial. Este recurso puede ser, por ejemplo, su acceso a Internet que desea compartir previo pago. Es frecuente que los nodos de una MANET, por su carácter móvil,

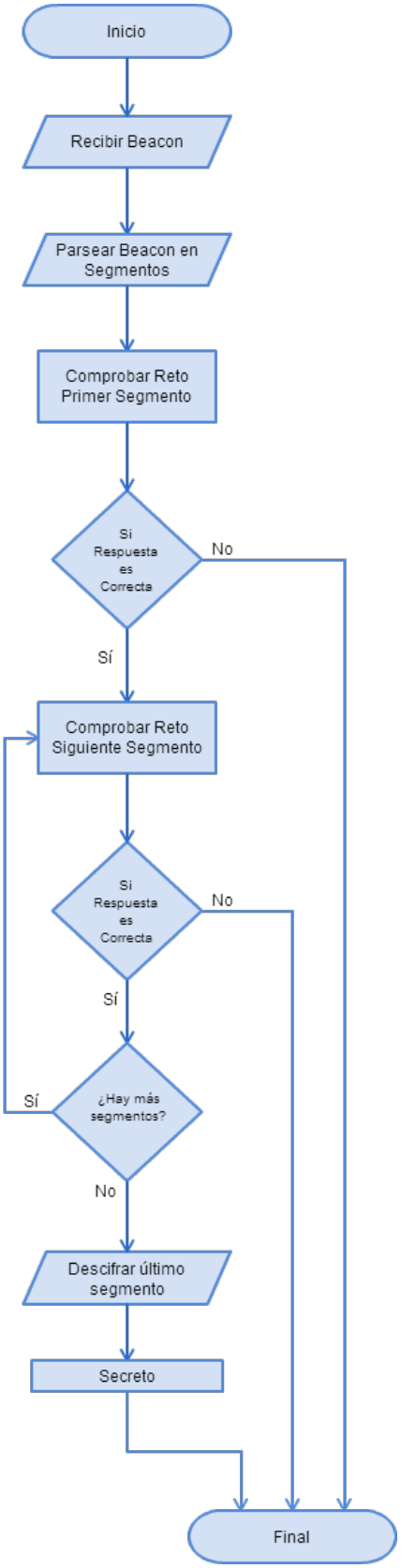

Figura 3. Diagrama de flujo del Algoritmo propuesto.

no posean acceso a Internet en muchos lugares. Un nodo legítimo de esa MANET que sí posea una conexión a Internet, puede tener como misión la comercialización de su conexión para que otros nodos legítimos hagan uso de ella. Esos nodos móviles que quieran hacer uso de esta conexión a la red de redes durante un tiempo limitado, sólo deben establecer una clave secreta de sesión compartida con el nodo emisor para comenzar las comunicaciones que le otorgan acceso a Internet. Para el establecimiento de las claves secretas de sesión se puede utilizar el esquema propuesto en este trabajo.

Otros dos escenarios diferentes para la utilización de dos variantes del esquema propuesto pueden ser para nodos legítimos de la red a los que sólo les interese notificar información de manera autenticada y unidireccional a otros nodos legítimos sin necesidad de usar claves secretas, y para nodos legítimos de la red que quieran compartir su clave pública de forma autenticada con otros nodos legítimos.

Por una parte, un nodo puede sólo desear hacer broadcast (ver Figura 2). De esta manera, otro nodo de la red que lo escuche, podrá fiarse de la información que quiere transmitir el nodo emisor ya que para confeccionar el beacon que se envía en modo broadcast es necesario conocer una clave secreta de red, que es utilizada para generar los grafos isomorfos y soluciones del protocolo descrito. Un ejemplo de caso de uso en este nuevo escenario es el de la notificación de eventos dentro de una VANET. Estos eventos que se envían en modo broadcast por parte de un usuario legítimo, pueden ser eventos de publicidad. Los distintos nodos de la red pueden recibir publicidad acerca de comercios que se encuentran cercanos a su ubicación y que también pertenezcan a la red. Para la retransmisión de esta publicidad se puede utilizar el esquema que se propone en este trabajo con el fin de que sólo los nodos legítimos de la red puedan enviar publicidad, evitando así el spam masivo de nodos que no pertenezcan a la red.

Por otra parte, un nodo puede querer anunciar su clave pública de forma autenticada sólo a aquellos nodos que también pertenezcan a la red. Para ello utilizará una variante del esquema propuesto (ver Figura 2), mediante la cual envía beacons periódicos que en su último segmento esconden la clave pública de ese nodo. Esto conlleva que sólo los usuarios legítimos de la red puedan acceder al último segmento del beacon, que contiene la clave pública del emisor, ya que los retos y respuestas están basadas en una clave secreta de red. La retransmisión de la clave pública en la que se basa este escenario puede servir para cualquier caso de uso de firma digital en MANETs ya que un usuario legítimo podrá enviar su clave pública a otros usuarios legítimos de la red de forma autenticada con objeto de posibilitar el uso de un esquema de firma digital en la MANET.

V. Conclusión

Con la proliferación de dispositivos electrónicos en múltiples ámbitos ha surgido un nuevo paradigma denominado Internet de las Cosas. Una de las mayores amenazas de un despliegue del tipo de redes que intervienen en IoT es la seguridad de las comunicaciones. Los objetos interconectados en IoT

suelen tener menos capacidad de cómputo que un ordenador convencional y sus comunicaciones suelen ser inalámbricas. Por este motivo se hacen necesarios nuevos algoritmos criptográficos ligeros que se adapten a estas características. En este trabajo, se presenta un nuevo esquema basado en la idea de las demostraciones de conocimiento nulo no interactivas en las que sólo es necesario el envío de un mensaje para compartir información confidencial. Como resultado del nuevo esquema propuesto se define su uso para el establecimiento autenticado de claves de sesión secretas entre pares de nodos legítimos de redes móviles ad-hoc. Además, el esquema que se ha diseñado puede ser utilizado por nodos que quieren enviar información autenticada en modo broadcast hacia otros nodos legítimos de la red. También se definen casos de uso para el intercambio autenticado de claves públicas en estas redes usando una variante del esquema que se propone en este trabajo. En definitiva, la nueva propuesta permite diseñar un nuevo protocolo basado en la idea de demostración de conocimiento nulo no interactivo en el que sólo es necesario el envío de un único mensaje en un sólo sentido.

Actualmente se está realizando la implementación del esquema propuesto en dispositivos móviles con objeto de analizar su comportamiento en entornos reales. Además su harán simulaciones en MANETs con diferentes configuraciones para estudiar la escalabilidad de la propuesta.

AGRADECIMIENTOS

Investigación financiada por el MINECO y la fundación FEDER mediante los proyectos TIN2011-25452 e IPT-2012-0585-370000, y la beca de investigación BES-2012-051817.

REFERENCIAS

[1] L. Atzori, A. Iera, G. Morabito, "The Internet of Things: A survey," *Computer Networks*, 2010.

[2] G. Bertoni, J. Daemen, M. Peeters, G. Van Assche, "Keccak sponge function family main document," *Updated submission to NIST*, Round 2, version 2.1, 2010.

[3] G. Bertoni, J. Daemen, M. Peeters, G. Van Assche, "The Keccak SHA-3 submission," *http://keccak.noekeon.org/Keccak-submission-3.pdf*

[4] P. Caballero-Gil, C. Caballero-Gil, J. Molina-Gil, C. Hernández-Goya, "Self-organized authentication architecture for Mobile Ad-hoc Networks," *WiOpt*, pp 217–224, 2008.

[5] C.L. Chen, C.T. Li, "Dynamic Session-Key Generation for Wireless Sensor Networks," *EURASIP Journal on Wireless Communications and Networking*, 2008.

[6] T. Eisenbarth, S. Kumar, C. Paar, A. Poschmann, L. Uhsadel, "A Survey of Lightweight-Cryptography Implementations," *IEEE Design and Test of Computers*, vol. 4, no. 6, pp 522–533, 2007.

[7] P. Ekdahl, T. Johansson, "A New Version of the Stream Cipher SNOW," *Proceedings of SAC, LNCS 2595*, pp 37–46, 2003.

[8] P. Ekdahl, T. Johansson, "SNOW - a new stream cipher," *Proceedings of NESSIE Workshop*, 2000.

[9] ETSI/SAGE, "Specification of the 3GPP Confidentiality and Integrity Algorithms UEA2 and UIA2. Document 2," *SNOW 3G Specification*, version 1.1, Septiembre 2005.

[10] U. Feige, A. Fiat, A. Shamir, "Zero-knowledge proofs of identity," *Journal of Cryptology*, vol. 1, Issue 2 , pp 77–94, 1988.

[11] M.R. Garey, D.S. Johnson, "Computers and Intractability: A Guide the theory of NP-Completeness," *Freeman and Co.*, 1979.

[12] O. Goldreich, S. Micali, A. Wigderson, "Proofs that yield nothing but their validity or all languages in NP have zero-knowledge proof systems," *Journal of the ACM*, 38(3), pp 690-728, 1991.

[13] S. Goldwasser, S. Micali, C. Rackoff, "The knowledge complexity of interactive proof systems," *SIAM Journal on Computing*, 18(1), pp 186-208, 1989.

[14] J. Groth, "Short Non-interactive Zero-Knowledge Proofs," *Advances in Cryptology - ASIACRYPT 2010*, pp 341–358, 2010.

[15] A. Martin, "On Some Symmetric Lightweight Cryptographic Designs," *Doctoral Dissertion, PhD*, Supervisors: T. Johansson, M. Hell, 2012.

[16] M. Toorani, A. Beheshti, "LPKI - A Lightweight Public Key Infrastructure for the Mobile Environments," *IEEE Singapore International Conference on Communication Systems*, pp 162–165, 2008.