CONGRESO DE JÓVENES INVESTIGADORES
Real Sociedad Matemática Española
Universidad de Murcia, del 7 al 11 de Septiembre de 2015

Esquemas Criptográficos en Redes Móviles Autogestionadas

Francisco Martín-Fernández[1], **Pino Caballero-Gil**[1], **Cándido Caballero-Gil**[1]

Con la aparición de la denominada Internet de las Cosas, donde la dimensión física se mimetiza con la dimensión lógica, es necesario codificar más de 100.000 millones de objetos, lo que equivaldría a que cada ser humano esté rodeado por 3000 objetos de media. Debido al carácter móvil y al reducido tamaño de muchos de estos dispositivos 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 y auto-gestión.

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.

Para paliar esto, en la bibliografía existen muchas propuestas [3], tanto basadas en criptografía simétrica [5] como en criptografía asimétrica [6]. 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 [2] aplicadas a la Internet de las Cosas [1], presuponer la existencia de un canal totalmente seguro para transmitir claves simétricas es una utopía. Además, el número de claves que se necesitan, es 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. El mayor inconveniente de los esquemas de criptografía asimétrica es su eficiencia computacional ya que en general los cálculos necesarios requieren bastante tiempo.

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 permite asegurar las comunicaciones inalámbricas en una MANET, tomando como base las pruebas de conocimiento nulo no interactivas. Las demostraciones de conocimiento nulo o ZKP (Zero-Knowledge Proof) [4] establecen un método para probar el conocimiento de un secreto sin revelar ninguna pista sobre él.

Referencias

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

[2] 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.

[3] 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.

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

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

[6] 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.

CONGRESO DE JÓVENES INVESTIGADORES
Real Sociedad Matemática Española
Universidad de Murcia, del 7 al 11 de Septiembre de 2015

[1]Departmento de Ingeniería Informática
Universidad de La Laguna
San Cristobal de La Laguna, S/C de Tenerife, España
{fmartinf, pcaballe, ccabgil}@ull.edu.es