Security mechanisms for Ad Hoc networks in urban environments

Enrique de la Hoz, Iván Marsá, Bernardo Alarcos

[1] Universidad de Alcalá, Departamento de Automática
28871 Alcalá de Henares, Spain
enrique@aut.uah.es, ivmarsa@aut.uah.es, bernardo@aut.uah.es

Abstract. Ad Hoc networks are a new communication paradigm whose application has been proposed in several environments because of their auto configuration capabilities and fast deployment. However, important challenges still remain, mainly related to security issues. In this paper, we propose the application of TESLA protocol for key distribution in an urban Ad Hoc network as the most appropriate alternative in the state of the art. Finally, we present some validation tests carried out using a preliminary stage implementation.

Mecanismos de seguridad para una red Ad Hoc en un entorno urbano

Enrique de la Hoz, Iván Marsá, Bernardo Alarcos

{enrique,ivmarsa,bernardo}@aut.uah.es

Resumen Las redes ad-hoc representan un paradigma de comunicación emergente cuya aplicación se ha propuesto en diversos entornos por su capacidad de autoconfiguración y rápido despliegue. Sin embargo, siguen planteados importantes desafíos relativos a problemas de seguridad. Uno de estos problemas es la gestión y distribución de claves. Se propone la aplicación del protocolo TESLA de distribución de claves a una red ad-hoc de servicios en un entorno urbano como la alternativa más adecuada frente a otras propuestas en el estado del arte. Finalmente, se realizan pruebas de validación de un estadio preliminar del algoritmo propuesto.

1. Introducción

Las redes ad-hoc constituyen un nuevo modelo de redes caracterizadas por la ausencia de una infraestructura fija subyacente y la posibilidad de autoconfigurarse, lo que permite un rápido despliegue de las mismas. Estas características de este tipo de redes las ha hecho muy atractivas para cierto tipo de aplicaciones tales como militares o aquellas en que es necesario un corto tiempo de establecimiento de red. Si a esto unimos la disponibilidad de dispositivos que trabajan en bandas frecuenciales libres podemos explicarnos el extraordinario interés que este tipo de redes han despertado de un tiempo a esta parte.

La mayor parte de los esfuerzos investigadores en redes ad-hoc han ido encaminados al desarrollo de protocolos de encaminamiento[1][2]. Sin embargo no se ha dedicado aún el esfuerzo necesario para afrontar los múltiples problemas de seguridad que plantean este tipo de redes. Así, junto a los mismos desafíos que se plantean en las redes convencionales, aquí tenemos que afrontar los derivados de la naturaleza inalámbrica de los enlaces, de la inexistencia de ningún tipo de entidad centralizada o infraestructura y de la movilidad de los nodos, teniendo en cuenta además el importante condicionante de la limitación de recursos que presentan los dispositivos que serán los nodos de esta red. Los problemas más importantes que han de ser afrontados en este tipo de redes[3] son la gestión y distribución de claves, el enrutamiento seguro y la detección de intrusiones.

En este artículo nuestro objetivo será centrarnos en presentar un mecanismo de distribución de claves basado en el protocolo TESLA orientado a la prestación de servicios de seguridad en una red ad-hoc dentro de un escenario urbano.

2. Gestión y Distribución de Clave

El servicio de encaminamiento seguro y los mecanismos de detección de intrusiones, así como la necesidad de proporcionar servicios de seguridad convencionales (autenticación, confidencialidad, integridad y no repudio), van a a requerir la utilización de técnicas criptográficas para poder ser ofrecidos. La utilización de uno u otro mecanismo criptográfico dentro de un entorno conlleva la necesidad de un servicio de gestión y distribución de claves para los algoritmos utilizados por los distintos elementos de la red. En el entorno de una red cableada convencional esto es abordado utilizando lo que se denomina una tercera parte de confianza (*Trusted Third Parties* o TTP), ya sea un centro de distribución de claves o una autoridad de certificación. Sin embargo, dentro de las redes ad-hoc, dada la inexistencia de infraestructura o de elementos centralizados, no vamos a poder trasladar dicho esquema tal cual sino que será necesario proponer alternativas que se adecúen a la naturaleza de las mismas.

Las líneas de investigación en la materia se dividen entre aquellas que proponen mantener el concepto de autoridad de certificación (CA), que en este caso sería ofrecido de manera distribuida entre una serie de nodos de la red y aquellas que descartan el uso de la CA y proponen un sistema completamente distribuido y autoorganizado de gestión y distribución de claves.

La primera propuesta [4,5] se basa en la distribución de la confianza de una CA entre un conjunto de nodos del sistema. Dicho conjunto, como una única CA, dispone de una clave pública y una clave privada. Todos los nodos conocen la clave pública y confían en todos los certificados firmados haciendo uso de la correspondiente clave privada. Cualquier nodo de la red puede, a su vez, actuar como cliente del servicio y solicitar la clave pública de cualquier nodo o actualizar su propia clave privada. El servicio de CA consta de n nodos a los que se denomina servidores cada uno de los cuales con su correspondiente pareja de claves pública/privada. Estos nodos almacenan la clave pública de todos los nodos de la red (servidores o no). Estos servidores utilizan criptografía de umbrales (*threshold cryptography*)[6] para ditribuir la capacidad de firma de certificados entre los n servidores. El sistema permite que hasta t servidores sean comprometidos sin que la capacidad de firma y la confianza en la CA tenga que verse afectada.

La segunda propuesta[7] no hace uso de una autoridad de certficación sino que distribuye el proceso de distribución de clave entre todos los nodos de forma similar a PGP. Esta es la propuesta del proyecto TERMINODES[8]. En este sistema cada usuario mantiene un repositorio local de certificados, en el cual almacena una serie de certificados de otros usuarios seleccionados por el usuario de acuerdo a algún algoritmo. Cuando un usuario u quiere conocer la clave de otro usuario v, los dos usuarios unen sus repositorios locales y el usuario u trata de encontrar una cadena de certficados apropiada de u a v en el repositorio conjunto así constituido. Los autores proponen algoritmos para la construcción de los respositorios locales que permiten, si son utilizados por todos los usuarios, el descubrimiento de dichas cadenas de certificados de uno a otro con una alta probablidad incluso en el caso de que el tamaño del repositorio local sea pequeño

en comparación con el número total de usuarios del sistema. Para ello utilizan un grafo, que ellos denominan grafo de confianza (a la manera de la malla de confianza de PGP) para representar las relaciones entre usuarios. Encontrar la cadena de confianza se reduce a encontrar el camino en el grafo que una el nodo que representa a u con el nodo que representa a v.

3. El protocolo TESLA

Este tipo de mecanismos serían necesarios para el establecimiento de claves para ser utilizadas por algoritmos que podrían ser utilizados para el establecimiento de canales que ofrezcan determinados servicios de seguridad entre dos nodos cualesquiera participantes en la red ad-hoc. Existen en el estado del arte otros protocolos que permiten la autenticación y protección de fujos broadcast o multicast como algunos de los propuestos en nuestro proyecto. El protocolo TESLA[9] es un protocolo de autenticación basado en difusión eficiente y empleado en entornos de redes ad-hoc[10]. TESLA protege los mensajes añadiendo un MAC a cada uno de los paquetes enviados autenticando por tanto las comunicaciones e impidiendo que se modifiquen o se generen paquetes falsos suplantando al emisor real. Tradicionalmente los protocolos de autenticación hacen uso de protocolos asimétricos como RSA para alcanzar sus objetivos. TESLA, sin embargo, hace uso de mecanismos de sincronización de relojes y de un método inteligente de generación y publicación de claves para ofrecer los mismos servicios que la criptografía asimétrica[11].

Para utilizar TESLA de cara a la autenticación, cada emisor genera una clave K_Ny genera una cadena de claves no reversible utilizando una función hash a partir del valor de comienzo:

$K_{N-1}= H(K_N)$, $K_{N-2}=H(K_{N-1})$...

Siguiendo este esquema cualquier nodo puede generar cualquiera clave K_i a partir de la clave $K_j$siempre que i >j. Este mecanismo permite verificar la validez de cualquier clave a partir de una clave anterior.

De cara a utilizar el protocolo, cada emisor planifica la publicación de cada una de las claves de la cadena anterior en orden inverso al de su generación. Esta temporización debe ser conocida por todos los nodos del sistema. El protocolo confía en la capacidad de un receptor para determinar qué claves debe haber liberado un emisor lo que requiere una cierta sincronización entre los nodos que podría ser alcanzada en un escenario muy abierto utilizando algún tipo de dispositivo GPS cada vez más común como accesorio en PDAs y teléfonos móviles. Para que el sistema pueda funcionar se debe acotar el máximo error de sincronización Δ entre dos nodos cualesquiera, y este valor debe ser comunicado a todos los nodos. Para enviar un paquete, el emisor determina un límite pesimista τ en el retardo máximo extremo a extremo de la red ad-hoc y elige una clave $K_i$de la cadena de claves tal que en ese instante el receptor piense que no ha sido publicada. Al enviar el paquete el emisor cálcula el MAC utilizando la clave K_iy lo añade al paquete. Cuando el paquete llega al receptor estamos en el

instante $t_S+\tau + \Delta$ y el receptor no aceptará el paquete si piensa que la clave puede haber sido publicada (en función del instante en que nos encontramos y la temporización anunciada) para evitar aceptar posibles falsificaciones del paquete. Dado que el receptor conoce que la desviación máxima del reloj del emisor Δ, rechazará el paquete a menos que se hubiera enviado al menos antes del tiempo esperado de liberación de la siguiente clave, con lo que el receptor debe poder verificar que la clave ha sido liberado al menos en el instante $t_S+\tau + 2\Delta$.

Cuando el receptor recibe un paquete autenticado con TESLA, en primer lugar verifica la condición de que la clave utilizada para autenticar el paquete no pueda aún haber sido liberada. Si la comprobación es exitosa, el receptor guarda el paquete y espera a que el emisor publique la clave K_i, cuando recibe K_i, la autentica y a continuación autentica los paquetes almacenados. El protocolo propone una función de derivación de claves a partir de las K_i, K'_i que serían las realmente utilizadas para autenticar los paquetes. Este algoritmo sería conocido tanto por emisores como por los nodos de la red.

TESLA sigue siendo seguro incluso en el caso en que el retardo extremo a extremo sea mayor que el supuesto, aunque en ese caso puede que algunos receptores puedan llegar a descartar el paquete.

4. Propuesta

En este artículo presentamos la posible adecuación de este modelo de distribución de claves a un escenario de redes ad-hoc dentro de un escenario urbano. En la actualidad nuestro grupo de investigación se encuentra trabajando dentro de un proyecto de provisión de servicios dentro de una red ad-hoc en un escenario urbano. En los entornos comerciales de las grandes ciudades el visitante o el ciudadano se ve abordado por una gran cantidad de ofertas comerciales, lúdicas o culturales. En la actualidad, el usuario no tiene nigún medio para filtrar de todas esas ofertas aquellas que pudieran resultarle de interés. Con el advenimiento de nuevos dispositivos como PDAs y teléfonos móviles es posible que si aportamos inteligencia a estos dispositivos sean éstos los que se encarguen de realizar el filtrado y la selección de esa información para nosotros. Si hacemos uso de las nuevas posibilidades de conectividad de estos dispositivos con una mínima inversión de comerciantes e instituciones bajo el modelo de red ad-hoc sería posible un rápido despliegue de la infraestructura de comunicación necesaria en ese entorno.

Si bien todas estas propuestas resultan atractivas es necesario solventar muchos inconvenientes desde el punto de vista de la seguridad en las comunicaciones que aparecen en un entorno de este estilo. Entre otros podemos resaltar la autenticación de los distintos emisores de información, la integridad y confidencialidad de las posibles transacciones que pudieran surgir como resultado del procesamiento de las ofertas y otras más comunes a otros escenarios de redes ad-hoc como la defensa de los nodos ante posibles intrusiones, los ataques de denegación de servicio que busquen dejar sin recursos y/o batería los dispositivos o la intercepción y reencaminamiento de mensajes.

Uno de los primeros riesgos que deben ser abordados es el concerniente a la recepción y verificación de información de los distintos oferentes de servicios. Así, tal y como comentábamos, podemos pensar en un escenario en que el ciudadano va recibiendo en su dispositivo portátil distintas ofertas por parte de distintos comerciantes, y es este dispositivo el que se va a encargar de filtrarlas y presentarlas al usuario en función, por ejemplo, de su coste. No es descabellado pensar que en un entorno de mucha competencia unos comerciantes intenten modificar las ofertas difundidas por los establecimienos vecinos con objeto de hacerlas menos atractivas y, por tanto,beneficiar sus propios intereses. Es posible incluso que unos comerciantes intentaran suplantar a otros para fabricar mensajes con ofertas que hicieran más atractiva la suya propia o incluso mensajes institucionales. Se plantea dentro de este tipo de escenarios que la PDA, en función de la información definida por entidades de promoción turística, calcule rutas para visitar los distintos monumentos. Esta información también podría ser maliciosamente alterada para hacer que la ruta preferida por los usuarios sea una y no otra favoreciendo la visita de ciertos establecimientos.

Los ejemplos anteriores muestran sin ningún género de dudas que es necesario la utilización de mecanismos que garanticen la integridad de los mensajes difundidos por las distintas fuentes, mensajes que por otra parte no tienen por qué ser confidenciales. Dentro de este escenario proponemos la utilización del protocolo TESLA para tal fin. Como hemos visto en la descripción del protocolo TESLA el objetivo primordial del mismo es la autenticación de mensajes de fuentes de difusión, que es exactamente el problema que acabamos de plantear. Cada uno de los posibles interesados en difundir este tipo de información aparecería en este esquema como un emisor TESLA que autenticaría sus mensajes utilizando el mecanismo descrito en el apartado anterior. Este procedimiento permite ofrecer el servicio de integridad sobre los mensajes de modo que el receptor tendría la garantía de que no han sido modificados y que proceden de la fuente alegada.

El protocolo TESLA tiene como requisito previo para poder ser utilizado una negociación entre emisor y receptores en la cual se establece el retardo máximo a utilizar, la temporización de las claves y la primera clave en ser liberada. Esta información debe ser autenticada por el emisor, por lo que es necesario que el sistema permita, en primer lugar, tanto la transmisión con los requisitos de seguridad anteriores de esa información como el reconocimiento de los distintos emisores TESLA válidos. Para el establecimiento de esta confianza se propone que sea una entidad centralizada la que se encargue de validar la lista de emisores autorizados. Para ello se propone la distribución a través de esta entidad, que en nuestro entorno podría ser el Ayuntamiento o la cámara de Comercio e Industria, de una lista de los emisores TESLA reconocidos firmada utilizando su clave privada RSA, o bien que el Ayuntamiento o la cámara se conviertan en Autoridades de Certificación que expidan certificados a los emisores autorizados y que sea a través de la validación de estos certificados como los nodos participantes puedan conocer de forma segura la clave pública del emisor TESLA y simultáneamente verificar que son emisores TESLA autorizados. Esto obliga a que los nodos participantes dispongan de la clave pública de esa autoridad

de certificación con anterioridad y de una forma segura. Esta clave podría ser distribuida o bien accediendo previamente a una web de alguna de estas instituciones desarrollada a tal efecto o en las oficinas de turismo de la localidad en la que estamos trabajando. Si se opta por la confección de una lista nuestro grupo propone un mecanismo estático en que sean estos participantes los que previamente se den de alta en la institución adecuada y sea esta institución la que se encargue de difundir la lista de emisores TESLA aceptados junto con una marca de tiempo para evitar que los comerciantes distribuyan listas validas pero pasadas con objeto de ocultar a posibles competidores. Cada uno de los emisores TESLA deberán disponer de un certificado X.509 que será emitido por una entidad certificadora propia y dependiente de alguna de las entidades que mencionaba anteriormente. Periódicamente, los emisores TESLA difundirán su certificado para que los posibles nodos cercanos puedan obtener su clave pública y así verificar la información necesaria para el comienzo de TESLA.

5. Pruebas y resultados

En estos momentos estamos trabajando en una maqueta del escenario real descrito en el punto anterior. La implementación concreta se ha realizado en Java y se ejecuta sobre una máquina virtual para la PDA IPAQ rx3700 utilizando como proveedor criptográfico *Criptix[12]* y con un PC funcionando como emisor TESLA puesto que suponemos que ese será el caso más habitual en el escenario objetivo. Se han realizado pruebas de validación de la aplicación así como de comprobación del funcionamiento de la misma en un entorno de red inalámbrica real donde el retardo de los paquetes extremo a extremo puede experimentar variaciones en función de la carga de la red y se ha comprobado que es posible la aplicación de este protocolo a redes reales con condiciones reales igualmente verosímiles. En la implementación hemos detectado que en función de la carga de la red se puede llegar a retardos que hacen que algunos nodos descarten claves válidas. Estamos trabajando en un mecanismos que nos permita adaptar el periodo de publicación de las claves TESLA dinámicamente en función de la carga de la red (en el protocolo original la duración de los intervalos es uniforme) para evitar que congestiones puntuales hagan superar el umbral τ que se establece para el retardo y por tanto que sean rechazadas claves válidas.

6. Conclusiones y trabajo futuro

Las redes ad-hoc representan un nuevo modelo de comunicaciones que, si bien abre una amplio abanico de posibilidades en muchos entornos diferentes, sigue presentando problemas serios en materia de seguridad que deben ser resueltos por los investigadores. Uno de estos problemas es el de la gestión y distribución de claves. Este proyecto adapta el protocolo TESLA para autenticar información emitida por difusión a la autenticación de mensajes en un entorno urbano real. La principal ventaja de la utilización de este protocolo frente a otras propuestas en el

estado del arte es su mayor sencillez y eficiencia al retirar carga de procesamiento de los nodos y al limitar al máximo la utilización de criptografía asimétrica.

Finalmente, hemos comprobado que, en un entorno y con una carga típica similar a la de un entorno real, que el protocolo sigue funcionando pese a las variaciones en el retardo de la red y que la carga extra derivada de la comprobación de paquetes es asumible en un dispositivo móvil medio.

Presentamos como aportación al protocolo el mecanismo de adecuación del calendario de publicación de claves en función de las condiciones cambiantes de la red para evitar que congestiones puntuales hagan que algunos nodos descarten información recibida válida.

Como líneas futuras, el objetivo final de nuestro grupo es hacer una propuesta de seguridad que cubra no sólo este sino otros posibles riesgos que aparecen en este entorno como el posible compromiso de los nodos, la seguridad en transacciones comerciales, la gestión de la confianza en otro usuarios o la detección de nodos comprometidos.

Referencias

[1] C. Perkins, E. Belding-Royer, S.Das. Ad Hoc On Demand Distance Vector (AODV) Routing, IETF RFC 3561, 2003.

[2] T. Clausen, P. Jacquet. Optimized Link State Routing Protocol, IETF RFC 3626, 2003.

[3] L. Zhou, Z. Haas, Securing Ad Hoc Networks, IEEE Network, 13(6):24-30, Noviembre-Diciembre 1999.

[4] Jiejun Kong, Petros Zerfos, Haiyun Luo, Songwu Lu and Lixia Zhang. "Providing Robust and Ubiquitous Security Support for Mobile Ad-Hoc Networks", Proceedings of tht IEEE 9th International Conference on Network Protocols (ICNP'01), pp. 251-260, 2001.

[5] Haiyun Luo, Songwu Lu, "Ubiquitous and Robust Authentication Services for Ad Hoc Wireless Networks", Technical Report UCLA-CSD-200030, Dept. of Computer Science, UCLA, 2000.

[6] Y. Desmeldt. "Threshold cryptography". European Transactions on Telecommunications, 5(4):449-457, Julio-Agosto 1994.

[7] Jean-Pierre Hubaux, Levente Buttyan, Srdjan Capkun, "The Quest for Security in Mobile Ad Hoc Networks", Proceedings of the 2001 ACM International Symposium on Mobile Ad Hoc Networking and computing, 2001.

[8] J. P. Hubaux, Th. Gross, J. Y. Le Boudec, and M. Vetterli, Towards self-organized mobile ad hoc networks: the Terminodes project, IEEE Communications Magazine, Enero 2001

[10] Yih-Chun Hu, A. Perrig, D.B. Johnson, Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks, Proceedings of the Sixth INternational Conference on Mobile Computing and Networking, 2002

[9] A. Perrig, R. Canneti, J. D. Tygar, and D. Song, TESLA: Multicast Source Authentication Transform Introduction, draft-ietf-msec-tesla-intro-04.txt, Diciembre 2004

[11] A. Perrig, R. Canneti, J. D. Tygar, and D. Song, The TESLA Broadcast Authentication Protocol, Cryptobytes Volume5, No. 2, 2002

[12] Cryptix Project Home Page. http://www.cryptix.org