UNIVERSIDAD Rafael Belloso Chacín

Revista Electrónica de Estudios Telemáticos

TÉLÉMATIQUE

REVISIÓN DEL PROCESO DE IDENTIFICACIÓN DE NODOS EN LAS WIRELESS SENSOR NETWORKS

(Authentication review for nodes in Wireless Sensor Networks)

Miguel Alfredo Acedo Arias[1]
María Aurora Molina Vilchis[1]
Ramón Silva Ortigoza[1]
Magdalena Marciano Melchor[1]
Edgar Alfredo Portilla Flores[1]

CIDETEC-IPN. Departamento de Posgrado. Área de Telemática.
Unidad Profesional Adolfo López Mateos. C.P. 07700, México, D.F., MÉXICO.
Correos electrónicos: macedo@ipn.mx, mamolinav@ipn.mx, rsilvao@ipn.mx, mmarciano@ipn.mx, aportilla@ipn.mx

RECIBIDO: julio 2008 APROBADO: Septiembre 2008

Resumen

La seguridad en las Wireless Sensor Networks (WSN) es una de las razones que están limitando su desarrollo e implementación práctica. Si bien los Mobile Transmission Elements (MOTE), núcleo de las WSN, han avanzado en capacidades de procesamiento y consumo de energía; las redes inalámbricas sin infraestructura que los soportan, hasta hoy, sólo han atendido aspectos básicos sobre los protocolos de ruteo requeridos, pero no así los protocolos de seguridad necesarios en el umbral entre las capas física y de enlace. De allí la necesidad de explorar el estado del arte de la seguridad en estas redes, enfocando los esfuerzos en la autenticación de nodos.

Palabras Clave: WSN, MOTE, autenticación de nodos

Abstract

Security in Wireless Sensor Netwoks (WSN) is one of the main reasons that are contributing to its underdevelopment and limiting their physical applications. While Mobile Transmission Elements (MOTE)'s processing capacities are growing and their power consumption is lowering; the Ad hoc networks that they use to complete their mission, they only had attend the basic aspects about data routing. Security protocols, between physical and data link layers, remain almost unattended. That is the reason why a state of the art study about security in WSN is justified, mainly if it is focus on node authentication.

Keywords*:* WSN, MOTE, node authentication

Depósito Legal: PPX200002ZU2142 / ISSN: 1856-4194. Volumen 8 Edición No 1 – Año 2009

INTRODUCCIÓN

Si bien la revolución de la computación estaba basada en la digitalización de la información para que ésta pudiera ser más fácilmente manipulada, la revolución inalámbrica que viene 0, se fundamenta en proporcionar información digital sobre todo aquello disponible, en cualquier lugar y a costos reducidos.

Los beneficios del mundo de la computación como la innovación en microcircuitos, ciclos cortos de desarrollo y bajo costo, han sido extendidos a las comunicaciones inalámbricas. Como resultado, cada vez más objetos se están conectando a todo tipo de redes, desde televisores y automóviles hasta maquinaria industrial o granjas completas 0. Con cerca de 10 mil millones de procesadores vendidos en el 2007 como parte de computadoras o enseres domésticos, la mayoría de estos dispositivos tienen la posibilidad de “pensar”, pero aún no pueden “hablar”, es decir, pueden realizar tareas específicas pero no comunicarse, sin embargo, esto está cambiando rápidamente.

De acuerdo con lo expresado por el Dr. David Clark, investigador del Massachusetts Institute of Technology (MIT) y uno de los creadores del concepto Internet, dentro de 15 ó 20 años la Internet albergará alrededor de 1 billón de dispositivos; la mayor parte con tecnología inalámbrica de algún tipo. Lo cierto es que de esa cantidad, sólo el 10% estará relacionado con el concepto actual de computadora, el restante 90% se referirá a pequeños dispositivos independientes o incorporados a objetos de uso cotidiano que establecerán el puente entre el mundo físico y el digital.

En un sentido amplio, la revolución que viene, proveerá de sentidos a lo que alguna vez solamente tuvo cerebro. Este será el papel que jugarán los sensores inalámbricos cooperando en redes de corto alcance con topologías dinámicas.

Este trabajo presentará en la segunda parte los elementos que conforman una Wireless Sensor Network (WSN), así como su arquitectura y las topologías que le son comunes. En la tercera parte se presentará el estado del arte de los protocolos de autenticación como mecanismo de seguridad para las WSN. Finalmente se presentarán las perspectivas que se vislumbran como evolución natural de esta tecnología y las direcciones que se pretende tomar en investigaciones futuras.

WIRELESS SENSOR NETWORK

Las redes inalámbricas de sensores o Wireless Sensor Networks están compuestas generalmente por un conjunto, que puede ser considerablemente grande, de dispositivos sensores autónomos de bajo costo, que están en comunicación vía una red inalámbrica de corto alcance. Los sensores al tener la capacidad de procesamiento y comunicación pueden ser introducidos en diferentes ambientes para que de forma cooperativa monitoreen variables físicas como temperatura, sonido, vibración, presión, movimiento o contaminantes 0.

Depósito Legal: PPX200002ZU2142 / ISSN: 1856-4194. Volumen 8 Edición No 1 – Año 2009

En 0) se describe una serie de funciones y características básicas de estas redes como la capacidad de auto organización. Siendo las más importantes la comunicación en difusión de corto alcance con ruteo multisalto. Alta densidad de nodos y esfuerzo cooperativo entre ellos. Cambios frecuentes de topología debido a las atenuaciones, fallas, retiro o adición de nodos. Limitaciones de energía, potencia de transmisión, memoria y poder de cómputo. De éstas, las últimas tres establecen la diferencia con las redes Ad hoc o la redes de malla.

Las tecnologías inalámbricas se pueden clasificar con respecto a la distancia que la señal puede alcanzar 0. Las señales que más viajan son las pertenecientes a los Global Positioning Systems (GPS) utilizadas por los sistemas satelitales, aunque son unidireccionales. Las señales de Worldwide Interoperability for Microwave Access (WiMax) con 5 Km de alcance y 15 Mbps ancho de banda; los celulares de tercera generación High Speed Downlink Packet Access (HSDPA) con 10 Km y 14 Mbps; los celulares de segunda generación Global System for Mobile (GSM) y Code Division Multiple Access (CDMA) con 35 Km y 400 Kbps, son las que siguen en alcance, además de utilizar enlaces bidireccionales.

En tercer lugar se tien las señales de corto alcance bidireccionales como Wireless Fidelity (WiFi) con 50-100 m y 54 Mbps y ZigBee con 30-100 m y 250 Kbps, este es el rango de las WSN. Un avance reciente en este rango, es la Ultra Wide Band (UWB) con un alcance de 5-10 m y 400 Mbps que usa frecuencias muy altas con un alcance de transmisión muy corto para transmitir grandes cantidades de información, como la transmisión de video de corto alcance. El cuarto tipo lo constituyen las Personal Area Network (PAN), el ejemplo típico es Bluetooth con 10 m y 700 Kbps. Por último, está la Near Field Communication (NFC) dónde el contacto debe ser próximo. Una variante la representa la Radio Frequency Identification (RFID) con 0.01-10 m y 1-200 Kbps. Por lo que en este panorama, lo anterior se ve resumido en la Figura 1.

	Tasa de intercambio por segundo	Rango	Costo USD**
WiMax móvil	15 Mb	5 Km	8
Red Celular 3G (HSDPA/LTE)	14 Mb	10 Km	6
Red Celular 2G (GSM/CDMA)	400 Kb	35 Km	5
Wi-Fi	54 Mb	50-100 m	4
Bluetooth	700 Kb	10 m	1
ZigBee	250 Kb	30 m	4
UWB	400 Mb	5-10 m	5
RFID	1-200 Kb	0.01-10 m	0.04

* Rendimiento típico, los datos actuales pueden variar
** Costo aproximado de los componentes en alto volumen

Fuentes: William Webb; Cambridge Consultants; OECD; Pyramid Research; Nokia; TI; CSR; Ember; Hitachi.

Figura 1. Rango de alcance de diversas señales de radiofrecuencia

En una red de sensores existen diferentes tipos de dispositivos, los cuales son identificados de acuerdo con las funciones que realizan dentro del sistema. Los estándares relacionados, como el estándar del Institute of Electrical and Electronics

Depósito Legal: PPX200002ZU2142 / ISSN: 1856-4194. Volumen 8 Edición No 1 – Año 2009

Engineers (IEEE) 802.15.4, distinguen los dispositivos basándose en la complejidad de su hardware y en sus capacidades 0. Dicho estándar define dos clases de dispositivos físicos: el Full Function Device (FFD) y el Reduced Function Device (RFD). La diferencia principal entre ambos es la cantidad de componentes que contiene cada uno de ellos y cuánta funcionalidad del estándar puede ser implementada.

Por lo que el FFD tendrá la cantidad de memoria y recursos necesarios para ejecutar todas las funciones y funcionalidades establecidas en el estándar. Incluso podrá asumir responsabilidades adicionales en el esquema de red, llegando a comunicarse con otro tipo de redes. Un RFD es un dispositivo de capacidades reducidas, para abatir costos y complejidad en los dispositivos. Típicamente contiene su interfaz física hacia el módem inalámbrico y ejecuta el protocolo de acceso al medio. Más aún, generalmente sólo se puede asociar con un FFD.

Basados en los FFD y RFD se pueden definir una serie de dispositivos lógicos. Los dispositivos lógicos se conforman de acuerdo con la combinación de las capacidades físicas y las responsabilidades que se les asigna en la red. En este sentido, se pueden definir tres categorías de dispositivos lógicos: el coordinador de red, el nodo ruteador y los dispositivos terminales o de término. El coordinador de red debe ser un FDD el cual tiene la responsabilidad de elegir los parámetros clave de la configuración de la red y el inicio de la misma. Al mismo tiempo puede almacenar información de la red y actuar como repositorio de llaves de seguridad.

El nodo ruteador debe ser un FDD que soporte la funcionalidad del ruteo de datos, incluyendo su actuación como interfaz para la interacción de diferentes componentes de la red y el paso de mensajes entre dispositivos remotos a través de caminos multisalto. Un nodo ruteador, puede comunicarse con otros ruteadores y con nodos terminales. Un dispositivo terminal es un RFD el cual contiene la funcionalidad justa para comunicarse con un nodo asignado, ya sea ruteador o coordinador. El dispositivo terminal no tiene capacidad de repetir mensajes.

Estos dispositivos lógicos pueden ser organizados de diferentes formas, originando tres tipos principales de topologías: estrella, malla o cúmulo en árbol, como se muestra en la Figura. 2.

Depósito Legal: PPX200002ZU2142 / ISSN: 1856-4194. Volumen 8 Edición No 1 – Año 2009

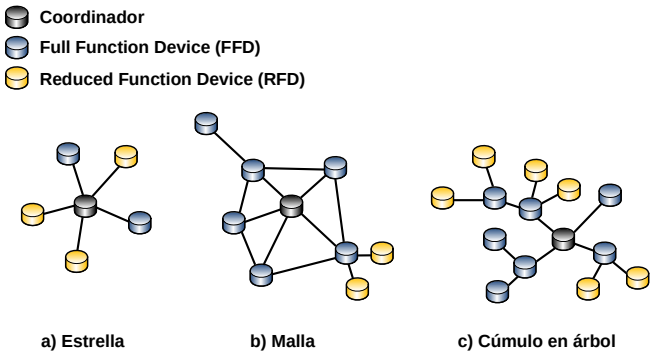

Figura 2. Topologías de red

La topología de estrella soporta un sólo coordinador como se ve en la Fig. 2(a), que para la IEEE 802.15.4 logra conectar hasta 65,536 dispositivos terminales. Todos los demás dispositivos son considerados como terminales o de término. El coordinador tiene la responsabilidad de iniciar y mantener en la red a los dispositivos terminales. Una vez inicializados, los dispositivos terminales solamente pueden establecer comunicación con el nodo coordinador.

Una topología de malla, ver Fig. 2(b), permite establecer caminos para la información desde cualquier dispositivo fuente a cualquier dispositivo destino, usando algoritmos de ruteo basados en tablas o árboles de ruteo. En la topología de malla se requiere que los radios de los nodos coordinadores y ruteadores estén encendidos todo el tiempo. Una red de cúmulo en árbol, Fig. 2(c), permite que se establezca una red punto a punto con un mínimo de proceso de ruteo, ya que usa el ruteo multisalto. Esta topología es ideal para aplicaciones con alta tolerancia a la latencia[1] en los mensajes. Otra de sus características es que se auto organiza y soporta la redundancia en la red, lo que permite un alto grado de resistencia a las fallas y adicionalmente se auto reparan.

El cúmulo puede ser significativamente grande, comprendiendo hasta 255 subcúmulos con hasta 254 nodos terminales en cada uno de ellos, para un total de 64770 nodos en la IEEE 802.15.4. Este tipo de topología puede abarcar áreas muy amplias. Cualquier FFD puede ser coordinador y solamente existe uno. El coordinador forma el primer cúmulo y le asigna un identificador o Cluster ID (CID) con valor cero. Los cúmulos subsecuentes son formados con una cabeza de cúmulo designada para cada uno.

Generalmente, cada red utiliza identificadores de 16 bits. En esta topología el nodo coordinador asume responsabilidades que incluyen el administrar la lista de

[1] En redes informáticas de datos se denomina latencia a la suma de retardos temporales dentro de una red. Un retardo es producido por la demora en la propagación y transmisión de paquetes dentro de la red 0.

Depósito Legal: PPX200002ZU2142 / ISSN: 1856-4194. Volumen 8 Edición No 1 – Año 2009

dispositivos asociados; el intercambio de tramas o paquetes de datos entre dispositivos de la red; la asignación de las direcciones de 16 bits, también conocida como dirección corta, a cada dispositivo de la red; generación de señales periódicamente para identificar el estado de la red así como los parámetros de los dispositivos asociados.

De acuerdo con **¡Error! No se encuentra el origen de la referencia.**) para cualquier uso práctico de las WSN la comunicación entre nodos no es suficiente. La red tiene que tener la capacidad de interactuar con otros dispositivos, por ejemplo aquellos conectados a Internet. Un escenario se muestra en la

Figura 3.

Desde este punto de vista, la WSN tiene la capacidad de intercambiar datos con un algún otro dispositivo móvil o con alguna clase de compuerta que le provea de la conexión física hacia Internet. Lo anterior tiene que ver con la capa física y la de enlace[2]. Independientemente de la topología utilizada en una WSN se requiere de una serie de servicios, como por ejemplo el acceso a otro tipo de redes. Pero la acumulación y el análisis de los datos no pueden ser realizados por los nodos sensores, sin importar el tipo físico al que correspondan, por lo que se requiere de una estación base que contenga las aplicaciones para tal propósito. La estación base también es utilizada para la configuración de la red y en algunos casos incluso de los nodos.

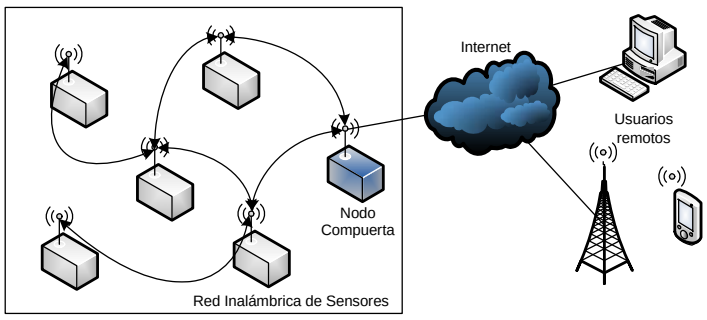

Figura 3. Una red WSN con un nodo como compuerta habilitando el acceso a clientes remotos vía Internet

La función de la compuerta, por otro lado, sí puede ser realizada por un FFD que contenga los programas necesarios. La asignación del nodo que tendrá esta función se puede identificar también de la Fig. 2. Para el caso de la topología en estrella Fig. 2(a), es obvio que será el nodo coordinador. Lo cual amplia las responsabilidades del mismo y le añade procesamiento, sin mencionar que hace a la red más vulnerable al

[2] Se refieren a las capas manejadas en el modelo de referencia OSI.

Depósito Legal: PPX200002ZU2142 / ISSN: 1856-4194. Volumen 8 Edición No 1 – Año 2009

tener sólo un elemento con todas las responsabilidades; la pérdida del mismo haría colapsar la red.

Para la topología de malla Fig. 2(b), la compuerta puede ser asignada a cualquiera de los nodos coordinadores, la selección final de su asignación pudiera estar relacionada con criterios de cercanía hacia la estación base o bien la fortaleza de la señal de un nodo coordinador con respecto de la red a la cual se quiere enlazar la WSN. En algunos casos, la responsabilidad podría ser dinámicamente asignada a los nodos coordinadores aludiendo a los criterios ya mencionados. Para una red en malla la pérdida de un nodo coordinador no significa el colapso de la red e incluso la función de compuerta puede ser relevada a otro nodo coordinador para mantener todas las funciones.

Para el caso de una red en clúster en árbol Fig. 2(c) la elección de la compuerta se basa también en la selección del nodo coordinador que llevará esta responsabilidad, una vez más se puede utilizar el criterio de cercanía hacia la estación base o la red alterna, sin embargo se debe tener en cuenta la jerarquía de los nodos coordinadores, por lo que sería preferible asignarla al nivel más alto de la jerarquía, es decir, el nodo coordinador con el CID más bajo. Al igual que en la red de malla, la pérdida de un nodo coordinador no significa el colapso de la red, a lo más una reorganización de la misma.

Con toda esta flexibilidad, características y funciones asociadas a las redes sin infraestructura y por herencia a las WSN, se podría pensar que no existen puntos débiles en ellas, situación que está muy lejos de la realidad. En 0) se identifican algunos de los retos y debilidades que deberán superar las WSN para convertirse realmente en ubicuas[3]. Algunas de las limitaciones de las WSN, sin circunscribirse a ellas, son los problemas de tamaño y capacidad de los nodos, factores de energía, costo de los nodos, cuestiones ambientales, en los canales de transmisión, la administración de la topología, su complejidad y la distribución de nodos, la implementación bajo estándares en lugar de soluciones propietarias, los problemas relacionados con la escalabilidad y problemas de seguridad.

Sin duda todos estos retos y debilidades son relevantes y deberán de ser superados, sin embargo no todos tienen el mismo peso o influencia para la adopción masiva de las WSN. Dependiendo de la aplicación, los aspectos de seguridad pueden ser los críticos 0. Las WSN deben habilitar la detección de intrusos y al mismo tiempo ser tolerantes a las fallas para proveer una operación confiable, aunque es común que los nodos sensores no estén protegidos en contra de manipulaciones o ataques.

En términos generales, de acuerdo con 0, la seguridad se define como la condición o cualidad de estar libre de preocupación, aprensión o ansiedad. Al ampliar

[3] La ubicuidad de las tecnologías está dada por la disponibilidad de servicios, procesos e información vinculada a ellas en cualquier lugar y en todo momento 0.

Depósito Legal: PPX200002ZU2142 / ISSN: 1856-4194. Volumen 8 Edición No 1 – Año 2009

el concepto hacia una red de comunicación, podemos establecer que una red segura es aquella en dónde sus usuarios no sienten algún tipo de aprensión o ansiedad mientras la usan. Nótese como el significado de una red segura depende de cómo es utilizada. Por ejemplo, mientras Internet fue del dominio de ingenieros y científicos, los usuarios no se preocuparon por la seguridad. Si el usuario era lo suficientemente diestro para acceder a ella, entonces podía usarla de la manera en que mejor le pareciera.

Con el advenimiento del uso comercial de la Internet, la seguridad se convirtió en todo un tema y al mismo tiempo en un campo de oportunidades. En esta línea de pensamiento, se considera que una red de comunicación segura debe de otorgar facilidades como la confidencialidad, integridad, autenticación, no repudio y confiabilidad en el servicio. Es crucial determinar que todas estas facilidades o requerimientos son estrictamente independientes, por lo que la presencia o ausencia de uno u otro(s) no garantiza la presencia o ausencia de otro(s). De esta forma, podemos establecer que un primer nivel de defensa en contra de algunas amenazas lo representan los mecanismos de autenticación en las WSN.

ESTADO DEL ARTE

Estudios en investigaciones recientes sobre las WSN coinciden en que los aspectos de seguridad son una prioridad en el desarrollo de esta tecnología 0. Al situarnos en el contexto histórico del desarrollo de las redes de comunicación, se puede identificar claramente el impacto e influencia que ha tenido el concepto Internet a nivel mundial. Sin embargo, como ya se ha mencionado, Internet estaba pensada para un contexto académico y de investigación; por lo que la seguridad pasaba a un segundo o tercer término, en el mejor de los casos. En una red que hoy día maneja alrededor de mil millones de dispositivos, sin duda la seguridad es una de las prioridades más importantes.

En 1992 El Dr. David Clark del MIT en una conferencia sobre temas técnicos relacionados con la denominación de dominios y su escalabilidad 0, mostró algunas diapositivas relacionadas con el lado obscuro de la Internet: su falta de seguridad inter construida. Hizo también referencia sobre la predisposición humana a ignorar los problemas, mencionando que los grandes desastres rara vez son causa de eventos súbitos y fortuitos; generalmente están asociados a procesos lentos e incrementales. “Las cosas se ponen peores lentamente. La gente se habitúa” señalaba en la presentación, “El problema es asignar el grado correcto de miedo a los elefantes a la distancia,” mostró en otra.

En una entrevista a finales del 2005 0 el Dr. Clark establece su creencia de que los elefantes están sobre nosotros, si bien la red ha traído consigo una serie de beneficios y maravillas tecnológicas, al mismo tiempo ha visto detenida su evolución como resultado de sus fallas en seguridad y en su habilidad reducida para acomodar nuevas tecnologías. El esquema actual de identificación de fallas, generación de remedios o parches y una vez más la identificación de fallas en un ciclo sin fin, es un

Depósito Legal: PPX200002ZU2142 / ISSN: 1856-4194. Volumen 8 Edición No 1 – Año 2009

esquema que no puede ser sostenido por más tiempo. Por lo que el Dr. Clark ha propuesto una nueva arquitectura para la Internet y redes colaborativas que contemplen desde un inicio otro tipo de elementos adicionales, como son: seguridad, protocolos, movilidad e instrumentación.

Con respecto a la seguridad la Internet debe autenticar a los equipos y personas que se comunican. Los nuevos protocolos deberán integrar mejores acuerdos de ruteo entre proveedores de servicios de Internet les permitirían colaborar en servicios avanzados sin comprometer sus negocios. Con respecto de la movilidad, el asignar direcciones del protocolo de Internet a dispositivos pequeños como sensores, teléfonos y procesadores inter construidos en automóviles les permitiría conectarse a la Internet de manera segura.

Por último, la instrumentación permitirá que todos los elementos activos de la red tengan la posibilidad y habilidad de detectar y reportar problemas emergentes a los administradores de las redes. Se puede deducir que el Dr. Clark identifica en sus trabajos, de manera indirecta, que dispositivos tan básicos como los sensores pueden contribuir de manera importante al caos existente en la red, más aún cuando él estima que en veinte años la cantidad de dispositivos en la red será de un billón. De los cuales, la mayoría serán dispositivos de capacidades reducidas como los sensores que conforman los nodos de las WSN.

La propuesta de mejoras en la arquitectura y la consideración de elementos de seguridad en nodos sensores o MOTES corresponde inicialmente a un grupo de investigación de la Universidad de California en Berkeley 0. En este trabajo no solamente se establece la propuesta de una arquitectura genérica para MOTES, al mismo tiempo presentan un prototipo y un sistema operativo basado en eventos que reside y funciona en el dispositivo. El sistema operativo denominado TinyOS, de un tamaño de 178 bytes, podía propagar eventos en el tiempo que le tomaba copiar 1.25 bytes a su memoria. Otro punto a resaltar, es que el documento es previo a las consideraciones del Dr. Clark y que en si mismo se constituye como el primer documento de uso público sobre los desarrollos y tecnologías de las WSN.

Al igual que el Dr. Clark, el documento mencionado, consideraba en el 2005 que una de las limitantes de la evolución de la Internet era su falta de seguridad, 0 coincide en que los aspectos de seguridad son también una de las causas por las que las aplicaciones prácticas de las WSN no se han dado a la fecha. Relacionado con los aspectos de seguridad en vehículos utilizando un esquema de autenticación con preservación de la identidad, este trabajo utiliza técnicas de firma ciega que permiten a los vehículos interactuar con infraestructura vial de manera anónima. Manifiestan al mismo tiempo que existen pocos trabajos que atiendan aspectos de seguridad como la privacidad y la autenticación en redes sin infraestructura.

Este trabajo está fechado a principios de 2008. El campo de la criptografía es el que se ocupa de dar solución a estas necesidades, lo cual da pie para poder establecer una clasificación de los artículos consultados. En una búsqueda exhaustiva

Depósito Legal: PPX200002ZU2142 / ISSN: 1856-4194. Volumen 8 Edición No 1 – Año 2009

y para fines de este trabajo, se identificaron 529 referencias sobre redes WSN, MANET y Ad hoc, el número total de referencias recuperadas para temas de seguridad en fueron 85, es decir, un 16% del que se identificaron los siguientes artículos relacionados con aspectos de autenticación en WSN, redes Ad hoc y Mobile Ad hoc Networks (MANET).

El 31% están relacionados con autenticación de llave pública 00, 21% con autenticación de secreto compartido 0, 10% con funciones hash 0, 10% con criptografía de umbral 0, 10% en esquemas de confianza 0 y el 18% restante en esquemas mixtos 0. De acuerdo con los datos estadísticos presentados, se coincide en que son pocos los trabajos relacionados con aspectos de autenticación para las WSN. En los párrafos siguientes se profundizará en lo expuesto en los trabajos seleccionados para establecer el estudio del estado del arte.

Debido a que este trabajo se centra en la autenticación, sería conveniente definir qué es y algunos conceptos relacionados. De acuerdo con 0 la palabra auténtico se refiere a algo que no es falso o una imitación, pero también es ampliamente aceptada la acepción relacionada con la veracidad de un hecho. La autenticación consiste de dos actos: el primero consiste en proporcionar pruebas de la autenticidad de la información que es enviada o almacenada, y el segundo, debe verificar las pruebas de autenticidad de la información recibida o recuperada.

La autenticación de un cliente significa que un cliente deseando obtener acceso a una red presenta su identidad con un conjunto de credenciales, como prueba de la autenticidad de la identidad presentada. Las credenciales son entonces usadas por la red para verificar que la identidad realmente pertenece a ese cliente. Intencionalmente se ha utilizado la palabra cliente, ya que la misma se puede interpretar como un dispositivo o un ser humano. Por esta razón, la autenticación de clientes debe ser dividida en dos categorías: autenticación de dispositivos y autenticación de usuarios.

Mientras que la autenticación de usuarios y dispositivos se encarga de asegurar que los actores en el proceso de comunicación son legítimos y quiénes dicen ser. La autenticación de los mensajes, por otra parte, se asegura de verificar la integridad de los datos. Es decir, la protección de la integridad de los datos tiene por finalidad prevenir el intento malicioso de corromper o modificar los datos de un mensaje. La autenticación es un mecanismo mediante el cual también se puede proveer o determinar privilegios, a esto se le llama autorización. El privilegio puede otorgar accesos a un recurso, como por ejemplo el acceso a un medio de comunicación, a una base de datos, a una computadora o a muchos otros servicios provistos por una red.

La eficiencia de una WSN depende de que los datos censados sean correctos. Al mismo tiempo, la seguridad es importante para prevenir que agentes externos (personas o dispositivos) puedan recuperar información correcta de ella. Se proponen los mecanismos de autenticación como contramedida de ataques internos y externos. La colaboración voluntaria entre nodos asume el acceso al medio, el descubrimiento

Depósito Legal: PPX200002ZU2142 / ISSN: 1856-4194. Volumen 8 Edición No 1 – Año 2009

de rutas y el reenvío de paquetes entre otros servicios. Cuando los nodos son autónomos, no quieren compartir información o son maliciosos en una red de gran escala, la suposición inicial deberá cambiar necesariamente. Por lo cual también es requerida la autenticación de los nodos.

En 0) se proponen dos protocolos para la autenticación entre sensores, uno directo y otro cooperativo. El directo utiliza un esquema estático y el cooperativo uno adaptivo. Ambos protocolos garantizan implícita y probabilísticamente la autenticación sin proceso significativo en los nodos con o sin la presencia de una estación base. El esquema de seguridad utiliza una técnica de generación pseudoaleatoria de llaves que usa el identificador del sensor como semilla. En 0 se presenta la problemática del uso de llaves de acuerdo para la autenticación en grupos dinámicos de pares. Se muestran cuatro propuestas de protocolos en fase inicial, por lo que las conclusiones se relacionan con la necesidad de llevar los protocolos a sistemas reales que provean de retroalimentación y experiencia para un mejor entendimiento de las necesidades y servicios de seguridad requeridos por grupos dinámicos de nodos.

El protocolo propuesto en 0) satisface tanto la autenticación como la confiabilidad de las comunicaciones en redes Ad hoc. El esquema de seguridad incluye el manejo de identidad anónimo, la imposibilidad del rastreo de la localización del nodo, llaves periódicas de una sola sesión, identidad pseudónima con autenticación implícita, entrada y salida dinámica de la red, inventario de sesiones en progreso y la encripción de los datos. La confiabilidad del protocolo incluye la tolerancia eficiente a ataques de negación de servicio o Denial of Service (DoS), tolerancia a fallas para recuperar mensajes perdidos y cambio de llave sin alterar las transmisiones de salida. En los autores arriba mencionados el común denominador es el uso de la tecnología de secreto compartido en los protocolos propuestos.

Una aproximación diferente de autenticación la encontramos en 0 que establece de manera categórica, en el 2001, que solamente puede usarse criptografía de llave simétrica en los nodos, debido a las limitantes de recursos en los mismos. Por lo que se propone un esquema de actualización periódica de llaves. Si bien el esquema propuesto, a decir de los autores, cumple con los requerimientos de seguridad y bajo procesamiento; la realidad es que la capacidad de los nodos aún es limitada, pero sin duda ha avanzado enormemente, sobre todo en el aspecto de procesamiento, por lo que el uso de criptografía asimétrica para esquemas de autenticación es viable actualmente.

Otra forma de atender la autenticación es mediante el establecimiento de mecanismos de confianza y reputación 0. El esquema habilita a cada nodo para asignar un valor de confianza a cada entidad con la que interactúa, el cual puede ser revocado. El proceso no requiere de mucho trabajo de cómputo y consume poca energía de transmisión por lo que lo hace ideal para las WSN. En esta misma aproximación, el trabajo de 0) innova al presentar un esquema de confianza evolutivo basado en la noción humana de la confianza; con interacciones iniciales de bajo riesgo y evolucionando hacia otras de mayor riesgo conforme el nivel de confianza

Depósito Legal: PPX200002ZU2142 / ISSN: 1856-4194. Volumen 8 Edición No 1 – Año 2009

aumenta. A diferencia del primero, éste último está pensado para reemplazar la intervención explícita de los humanos en escenarios aplicativos.

Las funciones Hash también forman parte de los procedimientos de autenticación en las redes y no es extraño que en 0) se plantee el uso de funciones Hash, es una aproximación de poco procesamiento computacional que no genera sobre proceso en los microprocesadores o microcontroladores de los nodos. En 0 se considera que las funciones Hash promueven la cooperación entre pares para todos los procesos de la red.

En tanto que en 0) las funciones Hash proveen la primera capa de seguridad de un esquema mixto, la cual es usada para la verificación del grupo y la rápida verificación de los mensajes. En la segunda capa de seguridad, se utiliza tecnología de secreto compartido, para una identificación segura de los nodos. Este esquema puede prevenir ataques internos y externos. Mientras que la primera capa provee seguridad limitada de baja complejidad, la segunda capa provee adicionalmente seguridad moderada de complejidad media.

Las autoridades de certificación en los esquemas de clave pública y la criptografía de umbral son otra forma de proveer los servicios de autenticación requeridos por las WSN. En 0 se propone utilizar autoridades de certificación distribuidas basadas en criptografía de umbral usando una arquitectura de clúster en árbol. Para el uso de este método, existen dos problemáticas principales: la localización de las Certificate Autorities (CA) y el cómo hacer la actualización de los certificados. El trabajo propone como solución utilizar el Clúster Head (CH) o nodo coordinador como CA, para que los nodos entrantes a la red tengan servicio y que el secreto compartido pueda ser actualizado de manera eficiente a través de la red.

Debido a que el control centralizado de grupos en redes Ad hoc conlleva inseguridades inherentes y al mismo tiempo es vulnerable a ataques internos y externos de la red. Descentralizar el control de acceso es un servicio de seguridad requerido en una red Ad hoc. No sólo para prevenir accesos no autorizados, también para el manejo de otros servicios como el manejo de llaves de seguridad y el ruteo seguro. Por lo anterior en 0 se propone un mecanismo de control de acceso basado en criptografía de umbral y más específicamente, con el uso de firmas electrónicas.

En 0 la característica sobresaliente del método propuesto es que se establece un número de llaves de umbral para las sesiones simultáneas entre el usuario y los nodos sensores, durante el proceso único de autenticación y sin el uso de llave pública criptográfica. El esquema reduce la complejidad computacional y al mismo tiempo refuerza los aspectos de seguridad. El trabajo hace dos contribuciones; un autómata y una autenticación de umbral con el manejo de llaves para defensa contra ataques externos.

Las WSN tienen problemas detectando y previniendo nodos maliciosos, los que usualmente acarrean amenazas y comprometen a los sensores a su alrededor. Como

Depósito Legal: PPX200002ZU2142 / ISSN: 1856-4194. Volumen 8 Edición No 1 – Año 2009

ya se ha mencionado, los nodos deben de soportar un servicio de autenticación para la identificación de los sensores y la transmisión de datos. La detección de intrusos permite también esquemas de prevención que amplían los mecanismos de seguridad para descubrir nodos maliciosos o comprometidos. En **¡Error! No se encuentra el origen de la referencia.** se propone un modelo de seguridad adaptivo para asegurar redes en topología de clúster en árbol.

El esquema permite que los nodos existentes en la red autentiquen a los nuevos, establecen canales seguros y un esquema de autenticación tipo broadcast[4] entre los nodos vecinos. Se previene la intrusión de nodos maliciosos usando los esquemas de autenticación. El esquema de seguridad es modular y el módulo de autenticación puede excluir nodos internos comprometidos, mediante el uso de alarmas, evaluación de la confianza y esquemas de listas blancas/negras. También en **¡Error! No se encuentra el origen de la referencia.** se argumentan y prueban la eficiencia en el protocolo con respecto de la seguridad, el consumo de energía, la cantidad de procesamiento y los procesos de comunicación.

En oposición a 0, más recientemente 0 han demostrado que la incorporación de criptografía de llave asimétrica es posible en las actuales condiciones de los nodos de las WSN. El esquema utilizado es el de llave pública con algunas variaciones. El trabajo en 0 propone una solución para emular de una manera dinámica y distribuida el papel de una Private Key Generator (PKG) en una WSN, de tal manera que los nodos que se unan puedan compartir la llave maestra de un esquema basado en identidad. La PKG se esparce de manera dinámica conforme la red crece.

El principal reto de una PKG en una red MANET o WSN es que no todos los nodos tendrían acceso a la misma de forma directa; ya que puede fallar durante el tiempo de vida del protocolo o incluso puede ser atacada, comprometiendo todo el sistema. Se propone el distribuir en una serie de nodos alternos el papel de PKG, de esta manera no habría un solo PKG en la red. Incluso nuevos elementos podrían serlo bajo ciertas circunstancias y requerimientos de hardware satisfechos. Adicionalmente, proponen un acuerdo de llaves en las contrapartes de manera no interactiva.

En 0, es más viable un sistema de autenticación multiusuario mediante broadcast el cual permite a muchos usuarios autenticarse y unirse a la WSN dinámicamente. Objeta que los mecanismos de llave pública proveen estos servicios pero no cumplen con la seguridad, escalabilidad y eficiencia simultáneamente. Para ello presenta un esquema de autenticación llamado Identity-based Multi-user Broadcast Authentication Scheme (IMBAS), basado en la identidad y un broadcast multiusuario. El broadcast lo dividen en dos categorías que emplean dos primitivas criptográficas diferentes. Los usuarios del broadcast se aseguran con una firma basada en identidad sin la necesidad de par (pairing-free); el emisor del broadcast es asegurado mediante una

[4] Broadcast, en castellano difusión, es un modo de transmisión de información donde un nodo emisor envía información a una multitud de nodos receptores de manera simultánea, sin necesidad de reproducir la misma transmisión nodo por nodo 0.

Depósito Legal: PPX200002ZU2142 / ISSN: 1856-4194. Volumen 8 Edición No 1 – Año 2009

firma Schnorr[5] con recuperación parcial de mensaje para optimizar la eficiencia. La llave privada de los usuarios es protegida mediante contraseña para resistir posibles ataques.

Como se ha descrito, para asegurar la interoperabilidad con redes actuales, se ha reutilizado mucha de la interacción entre cliente-servidor de las tecnologías de Internet con pequeños cambios para propiciar la comunicación entre pares que se da en la redes Ad hoc. Se desarrollaron métodos para el descubrimiento de servicios, manejo de sesiones y seguridad que puedan ser utilizados en redes sin infraestructura.

El marco de la arquitectura propuesto en **¡Error! No se encuentra el origen de la referencia.** habilita el uso seguro y dinámico de los servicios en redes Ad hoc. Se basa en tres piedras fundamentales: administración local de los dispositivos así como de la autorización y autenticación de los mismos, descubrimiento seguro de servicios y administración segura de las sesiones. Los cuales están presentes en el uso seguro de cualquier servicio y son tradicionalmente utilizados en las arquitecturas basadas en servidores. El marco utiliza un esquema de llave pública para la autenticación.

Una de la ventajas que se aprecian es que usuarios que se conocieron previamente se pueden autenticar entre ellos, aún si no hay una aplicación específica de por medio y toda la criptografía relacionada a la autenticación es realizada localmente. Un usuario o nodo debe tener la tabla de certificados de los demás usuarios o en su caso obtenerla de la red para luego verificarla de manera local.

Asegurar una red sin infraestructura de una manera completamente auto-organizada es efectivo y requiere de poco procesamiento, pero falla cumpliendo con la iniciación de la confianza, es decir, en la autenticación. La propuesta de 0 defiende que es necesario construir una relación de confianza bien establecida sin asumir nada y propone un modelo de confianza distribuida basado en una solución probabilística. Un negociador de “secreto”, secreto compartido, es utilizado solamente en la conformación inicial de la red, la cual evoluciona hacia relaciones con cadenas de confianza más robustas. Es entonces cuando un esquema de confianza auto organizado es adoptado como respuesta al cambio dinámico de miembros. El esquema está basado en criptografía de llave pública y su propuesta modular supone que el esquema puede ser extendido a protocolos de capas superiores.

El estudio de las redes Ad hoc está enfocando principalmente en retos específicos de la radiofrecuencia y en el ruteo de paquetes. Para que estas redes sean posibles y prácticas, también se tiene que considerar cómo es que interactúan los protocolos de Internet y cómo soportar sus aplicaciones en las redes Ad hoc o WSN. Por lo que 0 se enfocan en el descubrimiento de servicios, manejo de sesiones y seguridad para

[5] En criptografía, una firma Schnorr es una firma basada en la intratabilidad de ciertos problemas de logaritmos discretos. Está considerada como el esquema de seguridad más simple que puede considerarse seguro entre los modelos aleatorios, es eficiente y genera firmas cortas 0.

Depósito Legal: PPX200002ZU2142 / ISSN: 1856-4194. Volumen 8 Edición No 1 – Año 2009

estas redes. Adicionalmente se propone un módulo de autenticación y autorización (AA) que construye una estructura jerárquica de certificación que provee de derechos de acceso y niveles de seguridad a los usuarios. El esquema de control de acceso es de dos vías, los usuarios pueden definir diferentes derechos de accesos dependiendo de los servicios que los mismos proveen a los demás nodos, por lo que cada nodo de la red debe tener su módulo de AA.

La mayor parte de los protocolos de seguridad propuestos para WSN están diseñados para proveer un nivel uniforme de seguridad a lo largo de la red. Cuando un nodo se comunica, puede requerir de diferentes niveles de seguridad, basado en su rol o papel en la red. La propuesta de 0 es establecer un esquema de acceso basado en roles o papeles, llamado Role Based Access Sensor Network (RBASN) el cual provee de seguridad multinivel en la red. Cada grupo en la red es organizado de tal manera que se pueda implementar el esquema de roles.

La seguridad multinivel está basada en la asignación de llaves individuales para cada nodo de los diferentes niveles. La red se organiza mediante un diagrama Hasse[6] para calcular la llave de cada elemento y extenderla de manera que se pueda construir la llave de grupo. Se considera un protocolo óptimo en consumo de energía y velocidad de procesamiento. Se usa un modelo de certificación jerárquica con el manejo de llaves, para lo cual se sugiere el uso de llaves (públicas, privadas) en cada nodo, en lugar de sólo proveer una llave con un certificado adjunto a la llave para verificación en el control de acceso a la red.

En este modelo, se sugiere que la estación base cree las firmas digitales y las envíe al grupo de nodos que actuarán como autoridades de certificación y que generarán los certificados para los nodos terminales. Sugieren que el certificado sea creado con base en la localización del nodo y su jerarquía en la red.

Una aproximación aparentemente simplista se realiza en 0, ya que debido a las características de las WSN el trabajo se basó en localizar los esquemas de seguridad en la estación base. La aplicación implementa la mitigación contra el análisis de tráfico basada en la transmisión de paquetes encriptados. El rango de alcance de la red se extiende utilizando los nodos adyacentes como intermediarios y el modelo corrige algunos comportamientos irregulares de los nodos. En este caso, el procesamiento se realiza totalmente en la estación base y la participación de los nodos se limita al mínimo necesario. Este tipo de solución puede ser útil para redes de muy pocos elementos y con poco alcance, pero en definitiva es poco flexible, comparada con todos los esquemas propuestos con anterioridad.

[6] En matemáticas, un diagrama de Hasse es una representación gráfica simplificada de un conjunto parcialmente ordenado finito. Esto se consigue eliminando información redundante. Para ello se dibuja una arista ascendente entre dos elementos solo si uno sigue a otro sin haber otros elementos intermedios 0.

Depósito Legal: PPX200002ZU2142 / ISSN: 1856-4194. Volumen 8 Edición No 1 – Año 2009

La información y los datos en las WSN también pueden beneficiarse de técnicas de autenticación como los son las “marcas de agua” o watermarking 0. Las marcas de agua han sido propuestas para dos dominios generales: artefactos estáticos y artefactos funcionales. Los artefactos estáticos están compuestos únicamente de componentes que no son alterados durante su uso. Para este caso, las técnicas explotan la imperfección de la percepción humana. Los objetivos principales de las técnicas usadas en artefactos estáticos incluyen la incorporación de la marca de agua en el artefacto, la resiliencia contra su remoción y la posibilidad de una rápida detección de la misma.

Las marcas de agua en artefactos funcionales, como el software o el diseño de circuitos integrados, tienen como común denominador el que deben preservar en todo momento sus especificaciones funcionales, por lo que no utilizan los mismos principios que sus primos estáticos. Estos artefactos pueden ser especificados y por consecuencia “marcados” en diferentes niveles de abstracción; como por ejemplo las etapas de diseño esquemático, de síntesis lógica, de diseño físico o en su revisión funcional.

En las WSN, las marcas de agua o cualquier otra técnica de protección pueden ser implementadas en diferentes niveles del sistema, incluso el diseño de los nodos sensores y el software utilizado en la red pueden ser protegidos usando técnicas funcionales. Ambas técnicas estática y funcional, pueden ser aplicadas en la recolección de datos de la red dependiendo de las capacidades de sus nodos.

Adicional a los trabajos descritos, en 0, y relacionado directamente con redes MANET, se establece que los requerimientos de seguridad para cualquier infraestructura Ad hoc deben considerar al menos la seguridad en: los protocolos de enrutamiento, en la autenticación del acceso a través de la administración de claves y en sistemas de detección de intrusos, lo cual se puede observar en la Figura 4.

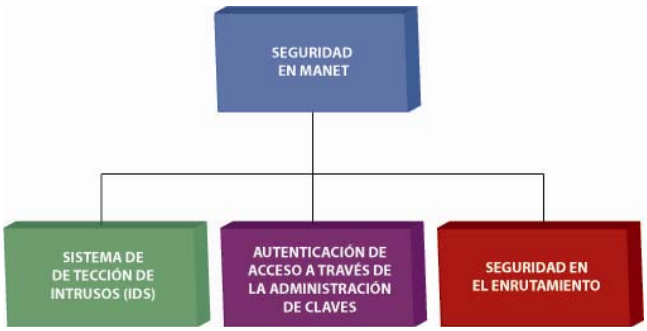

Figura 4. Modelos computacionales usados para la seguridad en redes MANET

Para 0 qué a su vez referencia a 0, se identifica que la tendencia de autenticación para redes MANET también tiene tendencias hacia los sistemas de llave pública en

Depósito Legal: PPX200002ZU2142 / ISSN: 1856-4194. Volumen 8 Edición No 1 – Año 2009

sus diversas modalidades, incluso algunos de ellos son muy similares a los ya descritos para redes WSN.

En la actualidad existen diferentes protocolos para la administración y distribución de llaves 0, muchos de ellos basados en un estándar ampliamente aceptado, como el algoritmo Diffie-Hellman. Ya que éste fue desarrollado para el dominio alámbrico de las redes, el mismo ha probado su inviabilidad computacional y en telecomunicaciones cuando se ha tratado de adaptar directamente a redes Ad hoc. Sin embargo, se observan mejoras significativas en 0 con su protocolo CLIQUES, y en el Tree-based Generalized Diffie-Hellman de (TGDH) 0, los cuales ya han podido ser implementados en algunas aplicaciones experimentales de redes Ad hoc.

La autenticación vía broadcast en las WSN tiene dos aproximaciones para 0 las firmas digitales y los esquemas basados en Timed Efficient Stream Loss-tolerant Authentication (TESLA). La UC Berkley en 0 utiliza µTESLA, una versión reducida de TESLA y el Secure Network Encryption Protocol (SNEP) para construir un esquema de seguridad bastante popular llamado Security Protocols for Sensor Networks (SPINS). Utilizando su experiencia en proyectos como SmartDust y al ser pioneros en esta tecnología, han logrado establecer un esquema completo de seguridad de alta eficiencia y de acuerdo con las limitaciones que presentan los MOTES.

Sin embargo, en Peng y Wenliang, (2008) se hace énfasis sobre las debilidades que tienen los protocolos de autenticación basados en broadcast, que entre otras, es que son vulnerables a ataques de negación de servicio. Proponen un mecanismo para mitigar este tipo de ataques llamado *message-specific puzzle.* El cual agrega un identificador en cada mensaje enviado, el cual puede ser fácilmente verificado por cualquier nodo, pero le tomaría a un atacante mucho tiempo y poder de cómputo para romperlo.

PERSPECTIVAS

Para trabajos futuros se pretenden analizar esquemas de seguridad basados en secretos compartidos bajo los esquemas de Shamir, conocimiento nulo, el Gamal y Brakley, ya que hasta el momento no se han considerado en las WSN, se debe evaluar su pertinencia considerando las limitaciones en prestaciones y energía de los nodos. Algunos de estos esquemas se consideran adecuados para las condiciones que presentan las topologías dinámicas de las WSN ya que son de fácil implementación y bajo consumo de recursos.

Tomando esto en cuenta, así como la resolución de los problemas de administración, distribución y revocación de certificados, que en las WSN implican la asignación de funciones especializadas en los nodos coordinadores, se puede llevar a cabo la implementación de esquemas criptográficos híbridos (asimétricos y simétricos). Adicionalmente, los sistemas híbridos con seguridad en capas o niveles pueden ser complementados con criptografía de flujo, especialmente Vernan, para

Depósito Legal: PPX200002ZU2142 / ISSN: 1856-4194. Volumen 8 Edición No 1 – Año 2009

encriptar las claves públicas o secretas con el uso de generadores de secuencias pseudo aleatorias.

CONCLUSIONES

La seguridad en las redes WSN es un tema que está cobrando importancia en la medida en que las aplicaciones experimentales de las mismas están haciendo su transición hacia la industria. Dadas las implicaciones de que tantos dispositivos pudieran estar en condiciones como los ya conectados a la Internet hoy día; se identifica claramente que contribuirían de manera definitiva a un caos generalizado. La seguridad, no contemplada de inicio en la Internet, es para las redes Ad hoc una condicionante para su éxito.

En ese sentido, los trabajos aquí mencionados aportan al orden que deberá prevalecer en las WSN si se quiere llevar las sensaciones de un mundo real a uno virtual. Lo cierto es que a la fecha no existen estándares para los MOTE y muchas de las tecnologías y protocolos asociados con ellos, por lo que los trabajos mencionados y muchos más, se están enfocando en dar claridad a este aspecto.

AGRADECIMIENTOS

M. A. Acedo-Arias: Agradece el apoyo recibido por el Programa de Año Sabático, de la Secretaría Académica del IPN.

M. A. Molina-Vilchis: Agradece el apoyo recibido por La Comisión de Operación y Fomento de Actividades Académicas (COFAA) y del Programa de Estímulo al Desempeño Docente (EDD).

R. Silva-Ortigoza:

E. A. Portilla-Flores: Agradece el apoyo recibido por La Comisión de Operación y Fomento de Actividades Académicas (COFAA), a la Secretaría de Investigación y Posgrado (SIP) del IPN, así como al Sistema Nacional de Investigadores (SNI-CONACyT).

M. Marciano-Melchor: Agradece el soporte económico recibido por la SIP-IPN, y del programa EDI.

REFERENCIAS

ATENIESE G., STEINER M., and TSUDIK G.. *New Multiparty Authentication Services and Key Agreement Protocols*. IEEE Journal of Selected Areas in Communications Vol. 18, No. 4, April 2000.

AVANCHA S., UNDERCOFFER J., JOSHI A., and PINKSTON J. *Secure sensor networks for perimeter protection*. Computer Networks 43.4:421-435.

Depósito Legal: PPX200002ZU2142 / ISSN: 1856-4194. Volumen 8 Edición No 1 – Año 2009

<http://www.sciencedirect.com/science/article/B6VRG-49DMVVH-1/2/8c336416ad2988ea2f3bdd9a7bca0d11>. 2003.

BASAGNI S., HERRIN K., BRUSCHI D., and ROSTI E.. *Secure pebblenets.* In Proceedings of the 2nd ACM international Symposium on Mobile Ad Hoc Networking &Amp; Computing (Long Beach, CA, USA, October 04 - 05, 2001). MobiHoc '01. ACM, New York, NY, 156-163. DOI= http://doi.acm.org/10.1145/501436.501438. 2001

BOUKERCH A., XU L., and EL-KHATIB K.. *Trust-based security for wireless ad hoc and sensor networks.* Computer Communications 30.11-12:2413-2427. <http://www.sciencedirect.com/science/article/B6TYP-4NNYJ99-1/2/bc3d7a31c831da427b521c2a1f367421>. 2007.

BURMESTER M. and DESMEDT Y. *Efficient and Secure Conference-Key Distribution*. In Proceedings of the international Workshop on Security Protocols (April 10 - 12, 1996). Lecture Notes In Computer Science, vol. 1189. Springer-Verlag, London, 1997. pp. 119-129.

CAO X., KOU W., DANG L., and ZHAO B. *IMBAS: Identity-based multi-user broadcast authentication in wireless sensor networks.* Computer Communications 31.4:659-667. <http://www.sciencedirect.com/science/article/B6TYP-4PYGVY3-1/2/ed70948fefb3742dec0b27b80c7eec99>. 2007.

CHANDRA P., *Bulletproof Wireless Security: GSM, UMTS, 802.11 and Ad Hoc Security.* Elsevier Inc. 2005. England. pp. 1-3.D. J. Beebe, “Signal conversion (Book style with paper title and editor),” in *Biomedical Digital Signal Processing*, W. J. Tompkins, Ed. Englewood Cliffs, NJ: Prentice-Hall, 1993, ch. 3, pp. 61–74.

DAZA V., MORILLO P. and RAFOLS C.. *On Dynamic Distribution of Private Keys over MANETs*. Electronic Notes in Theoretical Computer Science 171.1:33-41. <http://www.sciencedirect.com/science/article/B75H1-4NFS2PR-4/2/1d830220f6022af53125d8120994455e>. 2066.

DE MORAIS C. C. and PRAKASH D.. *Ad hoc & Sensor Networks. Theory and Applications.* World Scientific Publishing Co. Pte. Ltd. Singapur. 2006. pp. 524-550.

DI PIETRO R., MANCINI L.V., and MEI A.. *Random key-assignment for secure Wireless Sensor Networks.* In Proceedings of the 1st ACM Workshop on Security of Ad Hoc and Sensor Networks (Fairfax, Virginia). SASN '03. ACM, New York, NY, 62-71. DOI= http://doi.acm.org/10.1145/986858.986868. 2003.

DONG Y., SUI A., YIU S. M., LI V. O. K., and HUI L. C. K.. *Providing distributed certificate authority service in cluster-based mobile ad hoc networks.* Computer Communications 30.11-12:2442-2452.

Depósito Legal: PPX200002ZU2142 / ISSN: 1856-4194. Volumen 8 Edición No 1 – Año 2009

<http://www.sciencedirect.com/science/article/B6TYP-4NMC89M-1/2/6315e5e8e907baf77bb11270787c5816>. 2007

GRAY E., JENSEN C., O'CONNELL P., WEBER S., SEIGEUR J., and CHEN Y.. *Trust Evolution Policies for Security in Collaborative Ad Hoc Applications.* Electronic Notes in Theoretical Computer Science 157.3:95-111. <http://www.sciencedirect.com/science/article/B75H1-4K0N5H7-8/2/847fcc81380c5d0c4883574298caa0a3>. 2006.

HILL J., SZEWCZYK R., WOO A., HOLLAR S., CULLER D., and PISTER K. *System architecture directions for networked sensors*. In Proceedings of the Ninth international Conference on Architectural Support For Programming Languages and Operating Systems (Cambridge, Massachusetts, United States). ASPLOS-IX. ACM, New York, NY, 93-104. DOI= http://doi.acm.org/10.1145/378993.379006. 2000.

HOLGER K., *Protocols and architectures for wireless sensor networks.* John Wiley & Sons, Inc. 2005, England. pp.78-79.

HSIEH M.Y., HUANG Y. M., and CHAO H. C.. *Adaptive security design with malicious node detection in cluster-based sensor networks*. Computer Communications 30.11-12:2385-2400. <http://www.sciencedirect.com/science/article/B6TYP-4NKYNTN-1/2/43f2cebbc2854007b8843438f1df3068>. 2007.

ILYAS M., *Handbook of sensor networks: compact wireless and wired sensing systems.* CRC Press. 2004. United States of America. p. 31.

JIANG Y., LIN C., SHI M., SHEN X., and CHAU X.. *A DoS and fault-tolerant authentication protocol for group communications in ad hoc networks.* Computer Communications 30.11-12:2428-2441. <http://www.sciencedirect.com/science/article/B6TYP-4NMC89M-2/2/e5a50e2c612fe58beec4fd26485556ab>. 2007.

KALLSTROM L., LEGGIO S., MANNER J., MOKKONEN T., RAATIKAINEN K., SAARINEN J., SUORANTA S., and YLÄ-JÄÄSKI A.. *A framework for seamless service interworking in ad-hoc networks.* Computer Communications 29.16:3277-3294. <http://www.sciencedirect.com/science/article/B6TYP-4K4PVVY-2/2/f1b4349683858c1933cdef5530fd8139>. 2006.

KAZEM S., *Wireless sensor networks: technology, protocols, and applications.* John Wiley & Sons, Inc. 2007, England. p.29.

KIM Y., PERRIG A., and TSUDIK G. *Simple and fault-tolerant key agreement for dynamic collaborative groups*. In *Proceedings of the 7th ACM Conference on Computer and Communications Security* (Athens, Greece, November 01 - 04, 2000). CCS '00. ACM, New York, NY, 2000. pp. 235-244.

Depósito Legal: PPX200002ZU2142 / ISSN: 1856-4194. Volumen 8 Edición No 1 – Año 2009

LI C. T., HWANG M. S., and CHU Y. P.. *A secure and efficient communication scheme with authenticated key establishment and privacy preserving for vehicular ad hoc networks.* Computer Communications In Press, Corre: 140. <http://www.sciencedirect.com/science/article/B6TYP-4RDR1D5-1/2/f820bf252a6f25e310cd6375f4b6dc5b>. 2007.

MANNER J., LEGGIO S., MIKKONEN T., SAARINEN J., VUORELA P., and YLÄ-JÄÄSKI A.. *Seamless service interworking of ad-hoc networks and the Internet.* Computer Communications In Press, Uncor. <http://www.sciencedirect.com/science/article/B6TYP-4S08JW7-2/2/adedf69a000422a7c718ae7bbc37a899>. 2008.

MICROSOFT, *Tecnologías Ubicuas, la u-Sociedad. Administración de la Tecnología.* Microsoft. Centro de Información y Recursos para PyMEs [En línea]. Disponible en: http://www.microsoft.com/mexico/pymes/issues/technology/performance/usociedad.mspx [Consultado 25 Mayo 2008].

MOHAMMAD I., *Handbook of Sensor Networks: Compact Wireless and Wired Sensing Systems.* CRC Press. United States of America. 2005.

NAKHJIRI M., *AAA and network security for mobile access: radius, diameter, EAP, PKI, and IP mobility*. John Wiley & Sons, Inc. 2007, England. pp. 1-8.

PAN J., CAI L., SHEN X., and MARK J. W.. *Identity-based secure collaboration in wireless ad hoc networks.* Computer Networks 51.3:853-865. 2006.

PANJA B., MADRIA S. K., and BHARGAVA B. *A role-based access in a hierarchical sensor network architecture to provide multilevel security.* Computer Communications 31.4:793-806. <http://www.sciencedirect.com/science/article/B6TYP-4R0CKFP-3/2/9de9be8951fe9369d1625c09314d779c>. 2007.

PENG NING A. L. and WENLIANG D., *Mitigating DoS Attacks against Broadcast Authentication in Wireless Sensor Networks*. ACM Transactions on Sensor Networks, Vol. 4, No. 1, Article 1, Publication date: January 2008.

PERRIG A., R. SZEWCZYK J.D. TYGAR, V. WEN and D. E. CULLER, *SPINS: Security Protocols for Sensor Networks.* Wireless Networks 8, Kluwer Academic Publishers. Manufactured in The Netherlands. 2002. pp. 521-534.

PORTILLA J., *Wireless Sensor Networks.* Jorge Portilla [En línea]. Disponible en: the Centro Electrónica industrial Web site http://www.upmdie.upm.es/~jportill/Wireless_Sensor_Networks.html [Consultado 14 Abril 2008].

Depósito Legal: PPX200002ZU2142 / ISSN: 1856-4194. Volumen 8 Edición No 1 – Año 2009

REN K., LI T., WAN Z., BAO F., DENG R. H., and KIM K.. *Highly reliable trust establishment scheme in ad hoc networks.* Computer Networks 45.6:687-699. <http://www.sciencedirect.com/science/article/B6VRG-4C478S0-1/2/bb1cb860458142415ca6d4feb5dee24f>. 2004.

SAXENA N., TSUDIK G., and YI J. H.. *Threshold cryptography in P2P and MANETs: The case of access control*. Computer Networks 51.12:3632-3649. 2007.

SOHRABY K., MINOLI D., and ZNATI T., *Wireless sensor networks: Technology, protocols, and applications.* John Wiley & Sons, Inc. 2007, New Jersey. pp.178-181

SWAMI A., *Wireless sensor networks: Signal processing and communications perspectives.* John Wiley & Sons. England. 2007.

TALBOT D., and TECHNOLOGY REVIEW MIT, *Technology Review The Internet Is Broken.* Technology Review MIT. Consultado en abril 8, 2008, de http://www.technologyreview.com/Infotech/16051/?a=f. 2008.

TÉLLEZ C. C. F. *Detección de intrusos y seguridad en redes móviles Ad hoc,* Universidad Nacional de Colombia. 2006. Colombia.

THE ECONOMIST (a), The *coming wireless revolution. When everything connects,* Economist.com [En línea]. Disponible en: http://www.economist.com/opinion/displaystory.cfm?story_id=9080024 [Consultado 13 Marzo 2008].

THE ECONOMIST (b), *A world of connections,* Economist.com [En línea]. Disponible en: http://www.economist.com/specialreports/ displaystory.cfm?story_id=9032088 [Consultado 13 Marzo 2008].

THE ECONOMIST (c), *On the radio*, Economist.com [En línea]. Disponible en: http://www.economist.com/specialreports/displaystory.cfm?story_id=9032078 [Consultado 13 Marzo 2008].

TRIPATHY S., and NANDI S.. *Defense against outside attacks in wireless sensor networks.* Computer Communications 31.4:818-826. <http://www.sciencedirect.com/science/article/B6TYP-4PYGVY3-B/2/c49867cc55e25473e393d356409dd79d>. 2007.

TSAI Y. R., and WANG S. J. *Two-tier authentication for cluster and individual sets in mobile ad hoc networks.* Computer Networks 51.3:883-900. <http://www.sciencedirect.com/science/article/B6VRG-4KGPN13-1/2/85af86591e11f1a7adaa3f1b434d2cc5>. 2006.

Depósito Legal: PPX200002ZU2142 / ISSN: 1856-4194. Volumen 8 Edición No 1 – Año 2009

WIKIPEDIA (a), *Wireless sensor network.* Wikipedia, the free encyclopedia [En línea]. Disponible en: http://en.wikipedia.org/wiki/Wireless_sensor_network [Consultado 14 Abril 2008].

WIKIPEDIA (b), *Latencia.* Wikipedia, the free encyclopedia [En línea]. Disponible en: http://es.wikipedia.org/wiki/Latencia [Consultado 25 Mayo 2008].

WIKIPEDIA (c), *Broadcast (sobre IP)*. Wikipedia, the free encyclopedia [En línea]. Disponible en: http://es.wikipedia.org/wiki/Broadcast_%28Sobre_IP%29 [Consultado 25 Mayo 2008].

WIKIPEDIA (d), *Schnorr signature*. Wikipedia, the free encyclopedia [En línea]. Disponible en: http://en.wikipedia.org/wiki/Schnorr_signature [Consultado 25 Mayo 2008].

WIKIPEDIA (e), *Diagrama de Hasse*. Wikipedia, the free encyclopedia [En línea]. Disponible en: http://es.wikipedia.org/wiki/Diagrama_de_Hasse [Consultado 25 Mayo 2008]. <http://www.sciencedirect.com/science/article/B6VRG-4NB2WSK-2/2/c1b869ce7cab2618aa18f8828b1e142a>.

WONG, J. L., FENG J., KIROVSKI D., and POTKONJAK M. *Security in sensor networks: watermarking techniques. In Wireless Sensor Networks,* Kluwer Academic Publishers, 2004. Norwell, MA, pp. 305-323.

ZHANG Y. and LEE W. *Intrusion detection in wireless ad-hoc networks.* In *Proceedings of the 6th Annual international Conference on Mobile Computing and Networking* (Boston, Massachusetts, United States, August 06 - 11, 2000). MobiCom '00. ACM, 2000. New York, NY, pp. 275-283.

Depósito Legal: PPX200002ZU2142 / ISSN: 1856-4194. Volumen 8 Edición No 1 – Año 2009