Ciencia e Ingeniería Neogranadina
ISSN: 0124-8170
revistaing@unimilitar.edu.co
Universidad Militar Nueva Granada
Colombia

Acedo Arias, Miguel Alfredo; Molina Vilchis, María Aurora; Silva Ortigoza, Ramón; Marciano Melchor, Magdalena; Portilla Flores, Edgar Alfredo

ANÁLISIS DE LOS SECRETOS COMPARTIDOS PARA LA AUTENTICACIÓN DE NODOS EN LAS WIRELESS SENSOR NETWORKS MEDIANTE EL ALGORITMO DE SHAMIR

Ciencia e Ingeniería Neogranadina, vol. 18, núm. 2, diciembre, 2008
Universidad Militar Nueva Granada
Bogotá, Colombia

Ciencia e Ingeniería Neogranadina, Vol. 18-2, pp. 101-116. Bogotá, Diciembre 2008. ISSN 0124-8170

ANÁLISIS DE LOS SECRETOS COMPARTIDOS PARA LA AUTENTICACIÓN DE NODOS EN LAS WIRELESS SENSOR NETWORKS MEDIANTE EL ALGORITMO DE SHAMIR

ANALYSIS OF SECRET SHARING TO AUTHENTICATE NODES WITHIN WIRELESS SENSOR NETWORKS BY SHAMIR´S ALGORITHM

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

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

Fecha de recepción: *6 junio de 2008*
Fecha de aprobación: *15 de diciembre de 2008*

RESUMEN

Una nueva generación de redes está naciendo a partir de la evolución de dispositivos móviles de comunicación y de la convergencia de las diferentes tecnologías de redes en Internet. Estas son las denominadas redes Ad hoc, cuyas características imponen retos en el enrutamiento, administración eficiente de energía, seguridad, aplicaciones y estandarización. Las WSN (Wireless Sensor Network) son una clase especial de redes Ad hoc, en las que se manejan poblaciones numerosas de dispositivos sensores, describiendo topologías en malla dinámicas. Estas redes igual que Internet son objeto de múltiples ataques de suplantación de identidad realizados por usuarios maliciosos que persiguen objetivos diversos. En este artículo se presenta un protocolo de autenticación de nodos basado en el esquema de secretos compartidos de Shamir para una red de WSN con una población alta de nodos.

Palabras Clave: wsn, seguridad, autenticación, protocolo.

ABSTRACT

There is a new net generation that is growing up with the evolution on mobile communication and many Internet technologies. These nets are named Ad hoc and their characteristics challenge aspects like routing, power management, security, standardization and applications. The Wireless Sensor Networks are just a kind of Ad hoc networks that can handle numerous nodes in dynamic cluster tree topologies. Like Internet, these networks are a target for hackers' attacks. In this work we introduce a security protocol to authenticate nodes in WSN that is based on secret sharing technology from Shamir.

Keywords: wsn, security, authentication, protocol.

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 [5], 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 dispositivos se están conectando a todo tipo de redes, como los aparatos electrodomésticos, automóviles, maquinaria industrial, dispositivos de comunicación personal, etc. [6].

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, en una clase especial de redes Ad hoc, es decir las WSN (Wireless Sensor Network). No obstante, igual que las redes convencionales como Internet, serán sujetas a ataques por usuarios mal intencionados, motivados por diferentes objetivos que pondrán en riesgo la información que ahí se curse, causando daños importantes. La suplantación de identidades es uno de los muchos ataques que pueden presentarse en estas redes, comprometiendo la confiabilidad y disponibilidad de la red, es por ello que en este trabajo se propone un esquema de autenticación de nodos, en consideración de las bajas prestaciones computacionales con las que disponen estos dispositivos.

El esquema de secretos compartidos se ha usado para protocolos en redes como Internet, en servicios de apuestas y muchas otras en dónde la estrategia de seguridad es el requerir que varias entidades participen para la liberación del secreto o servicio, sin embargo en las WSN, dadas sus características y la gran cantidad de nodos que pueden estar involucrados, este esquema brinda la posibilidad de utilizarse para la administración de subredes o celdas empleando autoridades de confianza distribuidas

a lo largo de la topología. Adicionalmente, la simplicidad de la implementación del método numérico aporta en el ahorro de energía y es adecuado para la capacidad del tipo de microprocesadores o microcontroladores disponibles para los MOTE (Mobile Transmission Element).

Este trabajo presenta en la segunda parte los elementos que conforman las WSN, su arquitectura y topologías más comunes, así como las propuestas hechas para la autenticación de entidades. En la tercera parte se propone el análisis de un protocolo de autenticación de nodos basado en el esquema de secretos compartidos de Shamir. Finalmente en la cuarta parte se presentan las simulaciones del modelo propuesto para una red hipotética y se analizan los resultados de dicha simulación.

1. ASPECTOS BÁSICOS

Este manuscrito presentan los elementos que conforman las WSN, su arquitectura y topologías más comunes, así como las propuestas hechas para la autenticación de entidades. Luego se propone un protocolo de autenticación de nodos basado en el esquema de secretos compartidos de Shamir. Finalmente se presentan las simulaciones del modelo propuesto para una red hipotética y se analizan los resultados de dicha simulación.

1.1. WSN

Las WSN están compuestas generalmente por un conjunto que puede ser considerablemente grande, de dispositivos sensores autónomos de bajo costo, que se comunican vía enlaces de radio 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 ambientales físicas como temperatura, sonido, vibraciones, presión, movimiento o contaminantes [13, 16, 19]. Estas redes son capaces de organizarse, siendo esta una de sus características principales, para ello utilizan la comunicación en difusión de corto alcance con ruteo multisalto. Sin embargo presentan limitaciones de energía, potencia de transmisión, memoria y poder de cómputo. Estas limitaciones las diferencian de las redes Ad hoc o las redes de malla [8].

1.2. NODOS

En una red de sensores existen diferentes tipos de nodos, los cuales son identificados de acuerdo con las funciones que realizan dentro del sistema. Los estándares relacionados, como el estándar IEEE 802.15.4, distinguen los dispositivos basándose en

la complejidad de su hardware y en sus capacidades [15]. Dicho estándar define dos clases de dispositivos físicos: el Full Function Device (FFD) y el Reduced Function Device (RFD). Los nodos se definen en tres categorías: 1) coordinador de red, 2) nodo ruteador y 3) dispositivos terminales. 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. Mientras que un dispositivo terminal es un RFD que solamente contiene la funcionalidad justa para comunicarse con un nodo asignado, ya sea ruteador o coordinador, por lo que no tiene capacidad de repetir mensajes. Los nodos pueden ser organizados de diferentes formas, originando tres tipos principales de topologías: estrella, malla o cúmulo en árbol, como se muestra en la Figura 1.

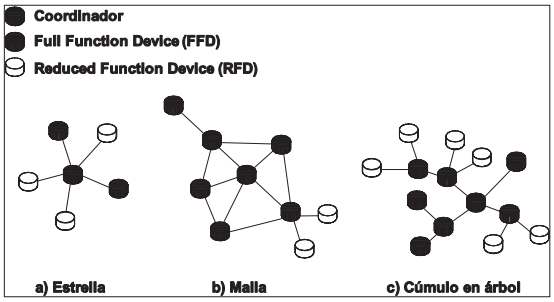

Figura 1. Topologías de red
Fuente: [15] SOHRABY, K., MINOLI, D. and ZNATI, T., (2007)

La topología de estrella soporta un solo coordinador como se ve en la Fig. 1(a), que para la IEEE 802.15.4 logra conectar hasta 65,536 nodos terminales. El coordinador tiene la responsabilidad de iniciar y mantener en la red a los nodos terminales. Una vez inicializados, dichos nodos solamente pueden establecer comunicación con el nodo coordinador. Una topología de malla, ver Fig. 1(b), permite establecer caminos para la información desde cualquier nodo fuente a cualquier nodo 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. 1(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 en los mensajes.

[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 [20].

De acuerdo con [7] para cualquier uso práctico de las WSN la comunicación entre nodos no es suficiente. La red tiene que tener la capacidad de interactuar con otras redes como por ejemplo a Internet o a las Local Area Network (LAN). Este escenario se muestra en la Figura 2. 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. Adicionalmente, una estación base sirve para ejecutar las aplicaciones de la red y también es utilizada para la configuración de la red y en algunos casos la configuración remota de nodos.

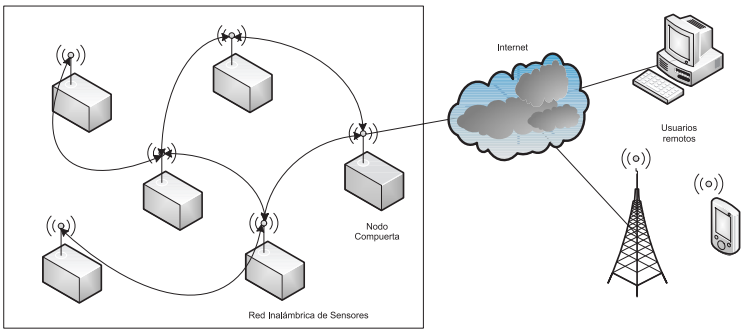

Figura 2. Red WSN con nodo como compuerta habilitando el acceso a clientes remotos vía Internet.
Fuente: [7] HOLGER, K., (2005)

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 [8] se identifican algunos de los retos y debilidades que deberán superar las WSN para convertirse realmente en ubicuas . 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, factores 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 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 aspectos más críticos [9]. 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.

[2] 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 [10].

1.3. AUTENTICACIÓN EN LA WSN

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 [1]. La autenticación consiste de dos actos: 1) proporcionar pruebas de la autenticidad de la información que es enviada o almacenada, 2) segundo, el acto de verificar las pruebas de autenticidad de la información recibida o recuperada. La autenticación de un nodo en la red significa que si éste desea obtener acceso debe realizar un proceso de identificación, la autenticación se encarga de asegurar que los actores (nodos) en el proceso de comunicación son legítimos y son quienes dicen ser.

Los nodos en la WSN colaboran entre sí por lo que el nivel de confianza requerido es alto, pero existe la posibilidad de que se introduzcan en la red nodos maliciosos que traten de afectar la información que se transmite entre ellos, esta suposición obliga a pensar en la necesidad de implementar protocolos o mecanismos de autenticación. No obstante en consideración de las prestaciones de hardware y de las limitaciones de energía con las que cuentan los nodos sensores, es requisito en el diseño de un esquema de autenticación el aprovechamiento eficiente de los recursos disponibles, por lo que los algoritmos de secretos compartidos, especialmente el de Shamir, parece ser una buena alternativa para implementar la autenticación de nodos.

1.4. SECRETOS COMPARTIDOS

Los secretos compartidos son algoritmos que generalmente vemos en aplicaciones de correo electrónico, votaciones electrónicas, juegos de azar, etc. No obstante pueden ser también implementados como protocolos de autenticación para las WSN [3]. En la actualidad existen diferentes protocolos para la administración y distribución de llaves, basados en Diffie-Hellman, un estándar ampliamente aceptado en las redes con infraestructura. Sin embargo, este protocolo es inviable computacionalmente y en las transmisiones cuando se ha tratado de adaptar directamente a redes Ad hoc. Sin embargo, se observan mejoras significativas en [1] con la propuesta del protocolo CLIQUES, y en el Tree-based Generalized Diffie-Hellman de (TGDH) [9], los cuales ya han podido ser implementados en algunas aplicaciones experimentales de redes Ad hoc, aunque todavía no en WSN.

Otro esquema importante de secretos compartidos es el de Shamir, que a diferencia del anterior se delega a una entidad central la generación y el procedimiento de compartición o división de los secretos. En este caso un secreto se divide en partes y se da a cada nodo a autenticar una sola de esas partes. De esta manera todas o algunas de esas partes sirven para reconstruir el secreto. El algoritmo de Shamir basa su funcionamiento en la propiedad de los nodos interpolares [14].

2. ALGORITMO ANALIZADO

Los protocolos criptográficos para compartir secretos tratan de resolver el siguiente problema: dado un secreto, repartir unos fragmentos de información entre varias personas, de modo que ciertas agrupaciones de estas personas puedan recuperar el secreto, pero las restantes agrupaciones no sean capaces de obtenerlo. Para describir matemáticamente este problema se considera:

$\mathcal{P} = \{P_1, ..., P_t\}$, el conjunto de *t* nodos que quieren compartir el secreto
$\mathcal{D} \notin \mathcal{P}$ *gestor* del esquema (entidad de confianza)
$\mathcal{K}$ un conjunto de secretos a repartir

$\Gamma \subseteq 2^{\mathcal{P}}$ el subconjunto de partes de $\mathcal{P}$ que determina qué conjuntos de participantes son capaces de calcular el secreto, a Γ se le denomina estructura de acceso y a sus elementos agrupaciones autorizadas. Un caso particular de estructura de acceso es el de los denominados *Esquemas Umbral,* representados mediante (l, t), los conjuntos autorizados son los que tienen al menos t participantes. Es decir, cualquier subconjunto de t o más participantes puede, uniendo sus particiones, recuperar el secreto, mientras que cualquier subconjunto con menos de t no puede hacerlo. S es el conjunto de participantes que se reparten, en particular, $S_i \subset S$ es el conjunto de participantes que puede recibir $\mathcal{P}_i$.

Adicionalmente, para la resolución del problema, en la Figura 3 se muestran para cuatro puntos la interpolation polinómica (cúbica), que es la suma de la bases polinómicas escaladas. La interpolación polinómica pasa exactamente por los cuatro puntos (llamados puntos de control) y cada base polinómica escalada pasa por su respectivo punto y se anula cuando x corresponde a los otros puntos.

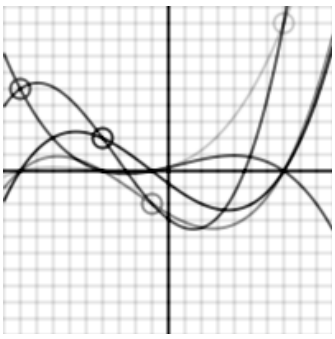

Figura 3. Interpolación polinómica cúbica
Fuente: [21] Wikipedia, (2008)

Por definición, se dice que el esquema es perfecto para realizar una estructura de acceso cuando se satisfacen las dos propiedades siguientes:

Si un subconjunto autorizado reúne sus participantes, entonces puede determinar el valor secreto de $\mathcal{K}$.
Si un subconjunto no está autorizado, entonces no puede determinar ninguna información acerca de $\mathcal{K}$.

Los esquemas de umbral cumplen con estas propiedades.

2.1. INTERPOLACIÓN DE POLINOMIOS

El método más simple de una interpolación polinomial es el método propuesto por Lagrange, el cual establece que siempre es posible construir un polinomio único $P_{n-1}(x)$ de grado $n - 1$ que pasa a través de n puntos distintos. El cual se obtiene de la *fórmula de Lagrange*

$$P_{n-1}(x) = \sum_{i=}^{n} y_i l_i(x) \quad (1a)$$

dónde

$$\ell_i(x) = \frac{x - x_1}{x_i - x_1} \cdot \frac{x - x_2}{x_i - x_2} \cdots \frac{x - x_{i-1}}{x_i - x_{i-1}} \cdot \frac{x - x_{i+1}}{x_i - x_{i+1}} \cdots \frac{x - x_n}{x_i - x_n}$$

$$= \prod_{\substack{j=1 \\ j \neq i}}^{n} \frac{x - x_j}{x_i - x_j}, i = 1, 2, \ldots, n \quad (1b)$$

son llamadas *funciones de cardinalidad*. Por ejemplo, si $n = 2$, el interpolante es una línea recta $P_1(x) = y_1 l_1(x) + y_2 l_2(x)$

Dónde

$$\ell_1(x) = \frac{x - x_2}{x_1 - x_2} \qquad \ell_2(x) = \frac{x - x_1}{x_2 - x_1}$$

Con $n = 3$, tenemos un interpolante parabólico: $P_2(x) = y_1\ell_1(x) + y_2\ell_2(x) + y_3\ell_3(x)$, en dónde ahora

$$\ell_1(x) = \frac{(x - x_2)(x - x_3)}{(x_1 - x_2)(x_1 - x_3)}$$

$$\ell_2(x) = \frac{(x - x_1)(x - x_3)}{(x_2 - x_1)(x_2 - x_3)}$$

$$\ell_3(x) = \frac{(x - x_1)(x - x_2)}{(x_3 - x_1)(x_3 - x_2)}$$

Las funciones cardinales son polinomios de grado *n-1* y tienen la propiedad

$$l_i(x_j) = \begin{Bmatrix} 0 \; si \; i \neq j \\ 1 \; si \; i \; = j \end{Bmatrix} = \delta_{ij} \qquad (2)$$

dónde δ_{ij} es la delta Kronecker.

Para probar que el polinomio interpolador pasa a través de los puntos, sustituimos $x = x$ en la ecuación (1a) y luego utilizamos la ecuación (2). El resultado es

$$P_{n-1}(x_j) = \sum_{i=1}^{n} y_i \ell_i(x_j) = \sum_{i=1}^{n} y_i \delta_{ij} = y_j$$

Se puede demostrar que el error de la interpolación polinomial es

$$f(x) - P_{n-1}(x) = \frac{(x - x_1)(x - x_2) \ldots (x - x_n)}{n!} f^{(n)}(\xi) \quad (3)$$

dónde ξ está en el intervalo (x_1, x_n); de otra forma su valor es desconocido. Otro punto a considerar es que entre más alejado esté el punto de x, más contribuirá al error en x.

2.2. ALGORITMO DE LA INTERPOLACIÓN POLINÓMICA DE LAGRANGE:

Entrada: Vector X con las abscisas de los puntos, valores enteros
Vector Y con las ordenadas de los puntos, valores enteros

Salida: L, matriz cuyos datos son los coeficientes del polinomio de interpolación de Lagrange
C vector con el polinomio de interpolación de Lagrange

1. w ← *longitud de X*
2. n ← *w - 1*
3. for k de 1 a n+1 hacer lo siguiente:
   a. V ← 1
   b. For j de 1 a n+1 hacer lo siguiente: $\left\{ \text{If k} \neq j \text{ entonces } V = \frac{convolución\left(V, polinomio\left(x(j)\right)\right)}{x_k - x_j} \right\}$

c. L(k,al final del vector) ← V

4. C ← $Y * L$

Nota: La función polinomio calcula las raíces de (X(j))

Algunas de las desventajas del uso de la interpolación polinómica de la forma Lagrange, de acuerdo con [20] son que debido a que se ajusta a todos los puntos que le son especificados, en situaciones con una gran cantidad de datos se obtienen polinomios de un grado muy alto, lo cual normalmente resulta impráctico. Es por esta razón que en la práctica no se utiliza, ya que se prefiere obtener polinomios de menor grado aunque los mismos no pasen por ninguno de los puntos que le son especificados, pero que se ajustan en forma aproximada siguiendo algún criterio de optimalidad. Otro de sus problemas es el sobre fiteo (overfitting) [3], es decir, a medida que crece el grado del polinomio interpolador, se percibe una creciente variación entre puntos de control consecutivos, lo que produce que la aproximación entre dos puntos continuos sea muy distinta a la esperada. A pesar de estos problemas, para el propósito buscado en este trabajo, el primero de ellos es una de las cualidades que utilizó Shamir para proponer su esquema de secretos compartidos.

2.3. ALGORITMO DE SHAMIR

La idea básica de Shamir en [14] fue la de fragmentar un secreto entre varias entidades, cada una de las cuales recibe un fragmento del secreto. El secreto puede ser reconstruido sólo cuando un subconjunto autorizado de participantes reúne sus fragmentos. Para [17] la idea detrás de los sistemas de secretos compartidos (Shared Secret Systems) es la protección o la privacidad de la información, vía su distribución. Algunas de las aplicaciones de los SSS son las firmas colectivas digitales, la custodia de claves, el almacenamiento de información, etc., en los cuales un número de participantes desea coordinar sus actividades para obtener algún objetivo. Generalmente se asume que el distribuidor de los fragmentos es una entidad confiable y que los fragmentos son entregados de manera segura a los participantes. En la Figura 6 se muestra este esquema de manera gráfica.

En general, los esquemas de compartición de secretos de umbral están definidos por medio de algoritmos probabilísticos, en los que se considera como entrada al secreto, que es un elemento de un conjunto finito, y su salida son los fragmentos del secreto. Por otra parte, el secreto es recuperado con el *umbral* t, es decir, en el que al menos t fragmentos pueden recuperar el secreto; y si menos de t fragmentos son conocidos, entonces no se sabe absolutamente nada sobre el mismo (en el sentido teórico de la información). Shamir en [14] formalizó las nociones de *privacidad* y *exactitud* en los

esquemas de umbral. En su esquema propuso elegir un polinomio (aleatorio) de grado *t-1*, y la recuperación del secreto se basa en la interpolación polinómica de la forma de Lagrange, anteriormente explicada. En [17] se menciona que el problema de un (l,t)-esquema umbral Shamir lo resolvió utilizando el siguiente algoritmo:

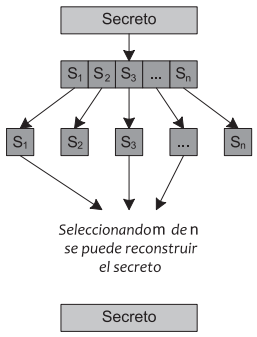

Figura 6. Sistema de secreto compartido

Fuente: [18] VÁZQUEZ, L., (2006)

Entrada: números enteros positivos l y $t \leq l$, y un secreto $\mathcal{K} \in \{0, \ldots, s-1\}$.

Salida: número enteros positivos fragmentos del secreto distribuidos en S_i

1. Se elige un número primo $p \geq max\{s, l+1\}$
2. Se eligen aleatoria e independientemente $a_1, \ldots, a_{t-1} \in \mathbb{Z}$
3. Se construye el polinomio de grado $t-1, q(x) = \mathcal{K} + \sum_{i=1}^{t-1} a_i x^i$
4. Se distribuye el secreto en las particiones $s_i = q(i) \in \mathbb{Z}, i = 1$

Los miembros del colectivo t podrán recuperar el polinomio q(x), puesto que conocen las imágenes de t puntos y en este polinomio el término independiente es el secreto. Ahora bien, t-1 miembros no obtendrían información adicional sobre la que ya tenían, ya que cualquier término independiente sería compatible con la construcción.

En una WSN, la estación base o bien un nodo coordinador pueden ejecutar el algoritmo para la distribución de secretos hacia los nodos adyacentes. Estos a su vez, se comunicarían hacia el origen cada vez que fuera necesaria una acción de autenticación, ya sea por la incorporación o eliminación de nuevos miembros dentro del espectro radioeléctrico o bien siguiendo políticas de seguridad. Cada miembro aportaría la parte del secreto que le ha sido confiada y al obtener el umbral en la estación fuente, se autenticarían todos aquellos que corresponden a la red. Bajo este esquema, cada nodo

coordinador, puede contener un número n de miembros bajo su influencia y a su vez estos ser parte de una red de nodos coordinadores hasta llegar al nivel de la estación base. Es bajo esta consideración que se presume adecuado para su aplicación en las WSN cuya estructura crece y se organiza de la misma forma.

3. RESULTADOS

Dada la generalidad propuesta por el algoritmo de Shamir, se decidió probar el mismo con un conjunto de datos aleatorios, con el objetivo de identificar sus debilidades. Al ejecutar el algoritmo de Shamir propuesto se solicita el secreto, el número de partes en que se va a dividir el mismo y el subconjunto de elementos requeridos para la reconstrucción del secreto, además de los coeficientes del polinomio. Estos últimos representan la fortaleza o debilidad del esquema, por lo que deben estar sujetos a una selección cuidadosa para mantener las propiedades del secreto perfecto.

El algoritmo funciona adecuadamente con número aleatorios, pero es conveniente que se construya el esquema de umbral eligiendo un número primo p mayor que el número mayor de partes en que se dividirá el secreto n, también llamadas sombras y mayor que el máximo secreto. Es entonces que se genera un polinomio arbitrario de grado n-1. Por ejemplo si se quiere generar un esquema de umbral (3,n), dónde l=3 es el número de sombras necesarias para reconstruir el secreto S de entre n entidades, esto se puede expresar como ($ax^2 + bx + S$).

Los coeficientes a y b se eligen al azar y se mantienen en secreto hasta la elaboración de las sombras, luego son descartados. Las sombras son obtenidas evaluando el polinomio en n puntos:

$$K_1=P(x_1) = P(1)\ ,\ K_2=P(x_2) = P(2),\ \ldots,\ K_n=P(x_n) = P(n)$$

Dado que el polinomio cuadrático P(x) tiene 3 incógnitas (a,b,S) hacen falta tres sombras o valores de P para resolverlas y recuperar el secreto S. Con dos valores no se puede y con más de tres sería redundante. Lo interesante del esquema es que cualquier subconjunto de 3 elementos que pertenezcan a n se pueden combinar para recuperar S. Con valores S=11 y un umbral (3,5) el programa calcula los siguientes valores para el polinomio $7x^2+8x+11$:

La simulación de MATLAB proporciona los siguientes resultados.

Introduzca el secreto: 11
¿En cuántas partes quiere dividir el secreto? (n): 5

```
Defina el número de elementos en el subconjunto (l): 3
Introduzca el cociente del exponente x^2:7
Introduzca el cociente del exponente x^1:8

ans =  7*x^2 + 8*x + 11
x =     1     2     3     4     5
y =     26    55    98   155   226
```

Con estos valores, en la segunda parte del programa, tomamos las duplas correspondientes a 2,4 y 5; y les aplicamos la interpolación polinómica de la forma de Lagrange. El resultado será el polinomio original:

```
Defina en el siguiente formato [1 2 ... n] los 3 puntos a considerar:[2 4 5]

xs =     2     4     5
ys =    55   155   226
L =
    0.1667   -1.5000    3.3333
   -0.5000    3.5000   -5.0000
    0.3333   -2.0000    2.6667
l = 7*x^2 + 8*x + 11
```

en dónde el término independiente del polinomio es el secreto.

4. CONCLUSIONES

En términos computacionales, el esquema de Shamir puede ser implementado en software de manera sencilla, requiere de poco poder de cómputo y consume poca energía en su procesamiento, de acuerdo con los resultados de la simulación presentada, lo que lo hace ideal, al menos en teoría, para aplicaciones en redes de sensores, debido a las limitaciones que se presentan en los MOTE.

Otra ventaja del esquema es que para topologías en clúster complicadas, la entidad generadora no necesariamente debe ser el nodo coordinador o la estación base. Un FFD puede realizar el trabajo para autenticar los RFD a su alcance. Los FFD a su vez pueden ser autenticados por el coordinador; en caso de más de un coordinador, estos pueden ser autenticados vía la estación base. De esta forma el esquema en el campo práctico nos brinda flexibilidad para redes con gran número de nodos, adicionalmente hay que notar que para este caso con diferentes entidades generadoras no necesariamente deben utilizar el mismo polinomio y secreto, e incluso estos pueden ser cambiados en el tiempo o de acuerdo con las condiciones de la red de manera dinámica.

Como trabajos futuros queda la evaluación de la complejidad computacional del algoritmo y las pruebas en escenarios de ataque para determinar su robustez en la WSN, así como su posible implementación en dispositivos físicos.

AGRADECIMIENTOS

MAAA: Agradece el apoyo recibido por el Programa de Año Sabático, de la Secretaría Académica del IPN.

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

RSO: Agradece el soporte económico recibido por la SIP-IPN, y del programa EDI y así como al Sistema Nacional de Investigadores (SNI-CONACyT).

EAPF: 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).

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

REFERENCIAS

[1] BURMESTER, M. and DESMEDT, Y. (1996), 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.

[2] DI PIETRO, R., MANCINI, L.V., and MEI, A., (2003), 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.

[3] DE MORAIS, C. and PRAKASH, D., (2006), Ad hoc & Sensor Networks. Theory and Applications. World Scientific Publishing Co. Pte. Ltd. Singapur. 2006. pp. 524-550.

[4] EARTH SYSTEM SCIENCE, (2008), An abbreviated glossary of system terminology. Earth System Science [En línea]. Disponible en: http://www.esse.ou.edu/glossary_st.html [Consultado 23 Agosto 2008].

[5] ECONOMIST, The, (2008), 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].

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

[7] HOLGER, K., (2005), Protocols and architectures for wireless sensor networks. John Wiley & Sons, Inc. 2005, England. pp. 78-79.

[8] KAZEM, S., (2007), Wireless sensor networks: technology, protocols, and applications. John Wiley & Sons, Inc. 2007, England. p.29.

[9] KIM, Y., PERRIG, A., and TSUDIK, G., (2000), 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.

[10] MICROSOFT, (2008), 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].

[11] MOHAMMAD, I, (2005), Handbook of Sensor Networks: Compact Wireless and Wired Sensing Systems. CRC Press. United States of America. 2005.

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

[13] PORTILLA, J., (2008), 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].

[14] SHAMIR, A., (1985), Identity Based Cryptosystems and Signature Schemes, Advances in Cryptography-CRIPTO 84, Lecture Notes in Computer Science, No. 196, Springer Velang, 1985.

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

[16] SWAMI, A., (2007), Wireless sensor networks: Signal processing and communications perspectives. John Wiley & Sons. England. 2007.

[17] TENA, J., (2003), Protocolos Criptográficos y Seguridad en Redes. Servicio de Publicaciones de la Universidad de Cantabria, 2003. España.

[18] VÁZQUEZ, L., (2006), Optimización de la eficiencia de los esquemas de compartición de secretos. Universidad Politécnica de Cataluña, 2006. España. pp. 2-4.

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

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

[21] WIKIPEDIA, (2008), Interpolación polinómica de Lagrange. Wikipedia, the free encyclopedia [En línea]. Disponible en: http://es.wikipedia.org/wiki/Polinomio_de_Lagrange [Consultado 15 Junio 2008].