Protocolo de autenticación para redes inalámbricas de sensores basado en identidad

Identity based authentication protocol for wireless sensor networks

Moisés Salinas Rosales[*]*, Gonzalo Duchén Sánchez*

ESIME Culhuacan, Instituto Politécnico Nacional, Av. Sta. Ana N.° 1000, 04430, Ciudad de México, México

(Recibido el 1 de abril de 2009. Aceptado el 23 de septiembre de 2009)

Resumen

En este trabajo se propone el primer protocolo de autenticación para redes de sensores usando criptografía basada en identidad, para lo cual se conjugan el uso de emparejamientos bilineales sobre un grupo de puntos en una curva elíptica y el uso de códigos de autenticación de mensajes. Dicho protocolo posee características que le permiten desarrollar tareas de autenticación de nodos y de mensajes, garantizando escalabilidad de la red y la diversidad de los nodos que la componen. Como parte de este trabajo se describe la propuesta detallada del protocolo, así como una estimación de sus costos de operación.

----- *Palabras clave:* Redes de sensores, criptografía, emparejamientos, autenticación, seguridad

Abstract

In this work, a novel identity based authentication protocol for sensor networks is proposed, involving bilinear pairings over an elliptic curve point group, and message authentication codes, as main underlying components. This protocol is capable to perform authentication for both nodes and messages, guarantying an acceptable level of scalability for network size and nodes' diversity. Herein, the proposed protocol is described in depth, as well the costs estimations for its operation on a WSN.

----- *Keywords:* Sensor networks, cryptography, pairings, authentication, security

* Autor de correspondencia: teléfono: + 52 + 55 + 565 62 058, fax: + 52 + 55 + 565 62 058, correo electrónico: msrosales@acm.org (M. Salinas)

Introducción

Las redes inalámbricas de sensores (WSN: Wireless Sensor Networks) son un caso particular de las redes ad-hoc; están compuestas por cientos o incluso miles de nodos, los cuales tienen el objetivo de trabajar en conjunto para realizar mediciones de eventos que ocurran dentro de su área de cobertura. Cada nodo es un dispositivo integrado por un micro-controlador, uno o más sensores y una unidad de radio-comunicación de muy corto alcance y baja potencia, alimentado con baterías, lo que define el tiempo de vida útil del sensor. La principal aplicación de las WSN es el monitoreo en sitio. Una de las primeras aplicaciones fue monitoreo de ecosistemas, el cual requirió evitar el uso de cableado para datos y energía con el fin de minimizar sus efectos invasivos, posibilitando la toma de mediciones como luz y humedad, a partir de la siembra de dispositivos sensores dentro del escenario a monitorear [1, 2]. Esta primera generación de aplicaciones no presentó requerimientos específicos de seguridad de la información y los esfuerzos de diseño estuvieron concentrados en el uso del canal inalámbrico, la extensión de la vida de la batería y la auto-organización de la red.

Como consecuencia de la flexibilidad de las WSN para su configuración y la posibilidad de detectar una gran variedad de eventos, surgió el interés en aplicar las WSN a otras tareas de monitoreo, donde la vigilancia humana hiciera inviable la medición ya sea por representar altos costos o incluso el riesgo de pérdida de vidas. Como ejemplos destacan el monitoreo de vibraciones en construcciones, el monitoreo de pacientes, así como aplicaciones de índole militar como la detección de accesos no autorizados a áreas físicas, la vigilancia de líneas fronterizas e incluso de condiciones del enemigo en los campos de batalla, tal como se describe en [3-5].

Esta segunda generación de aplicaciones de las WSN presenta requerimientos específicos de seguridad para la información en la red. Garantizar la autenticidad de la información es uno los más importantes, tal como se describe en [6]. La importancia de garantizar autenticidad en la WSN radica en evitar que un atacante interactúe con la WSN sin ser detectado, lo que pudiera derivar en un ataque a su seguridad. Uno de los posibles ataques es la falsificación de mensajes, la cual puede afectar los mensajes de datos, así como los mensajes de control de la red, pudiendo ambos casos resultar en el compromiso de la operación e incluso del control de la propia red. Un segundo ataque consiste en la suplantación de nodos, donde un nodo malicioso interactúa con la WSN ganando así acceso a la información e incluso también al control de la red. Para prevenir ambos ataques se requieren controles de autenticación, de mensajes para el primero, y de nodos para el segundo. Dichos controles, además de proteger a la WSN ante los ataques referidos, deberán atender a las necesidades específicas de cada aplicación, incluso aún en el caso de nodos recién integrados a la red.

La aplicación de controles criptográficos representa una solución al requerimiento de autenticidad; sin embargo, debe considerarse una adecuada selección de primitivas criptográficas con el fin de reducir al mínimo el efecto de sobre—costo para la red, mientras se mantienen las características de las WSN como la flexibilidad en configuración y topología, así como la escalabilidad en la densidad de nodos y el soporte a variaciones en las rutas de tráfico durante el tiempo de operación de las mismas. Actualmente el diseño de controles criptográficos para ambientes de redes de sensores es un área muy activa. Los primeros trabajos se enfocaron a la aplicación de técnicas criptográficas de llave simétrica, debido principalmente a su bajo costo computacional, y se pueden clasificar según el enfoque usado en: pre-distribución de llaves, distribución aleatoria de llaveros, distribución de llaves con base en ubicación y búsqueda de llaves en vecindarios, tal como proponen en sus respectivos trabajos Du [7] y Li [8]. Una segunda generación de trabajos se enfocaron al uso de criptografía de llave pública (PKC: Public Key Cryptography) en las WSN, en este rubro destacan las mediciones sobre los costos de este tipo de criptografía en ambientes limitados hechas por Wander [9] y las técnicas

de ahorro de energía reportadas por Uhsadel [10] y Szczechowiak [11]. Un camino alternativo a los certificados digitales para verificar la autenticidad de las llaves públicas es la propuesta por Du en [12], la cual consiste en sustituir las operaciones costosas de llave asimétrica, específicamente la verificación de firma digital, por un método basado en funciones hash y árboles de Merkle para verificar la autenticidad de las llaves. Por otro lado está la criptografía basada en la identidad, cuya exploración ha iniciado con algunas propuestas que hacen interesante su estudio en una WSN, en este rubro se destaca el trabajo de Oliveira [13], quien propuso un método para la distribución de llaves entre nodos.

En este artículo se propone un protocolo de autenticación para WSN basado en identidad, el cual explota las propiedades de bilinealidad de los emparejamientos a través de la aplicación del esquema de cifrado basado en identidad. El diseño propuesto retoma la idea de Du [12] de minimizar las operaciones costosas, para lo cual se desarrolla una estrategia que consiste en permitir a dos nodos cualesquiera autenticarse uno al otro, para verificar su pertenencia a la WSN, y posteriormente autenticar las comunicaciones entre dichos nodos. A continuación se describe el escenario de una WSN requiriendo los servicios de autenticación, seguido de una breve descripción de las herramientas criptográficas utilizadas y de una comparación del protocolo propuesto frente a otros trabajos en el área. Se elabora una descripción detallada del protocolo a través de sus diferentes fases, y se presentan sus principales características en términos de eficacia y eficiencia en costo como resultados. Finalmente, se incluyen las conclusiones del trabajo y se destacan posibles trabajos a futuro.

Metodología

Consideraciones para el diseño de un protocolo de autenticación para una WSN

El protocolo de autenticación propuesto en este trabajo tiene como objetivo establecer, de forma segura y autenticada, la comunicación entre dos nodos, para lo cual, la estrategia propuesta consiste en construir primero, una asociación de confianza entre los dos nodos, y luego proceder a autenticar sus comunicaciones. Para ello un primer nodo, forma ya parte de la red en operación y adopta el rol de *nodo autenticador*. Un segundo nodo pretende establecer un vínculo de conexión hacia la red de sensores a través del primero y adopta el rol de *nodo suplicante*; estos roles se adaptan con base en los principios de un sistema de autenticación. Este escenario puede presentarse a raíz de la agregación de nuevos nodos a la red o por la necesidad de un nodo para establecer nuevas rutas como consecuencia de cambios en la topología. Para disminuir los costos de autenticar mensajes con firmas digitales u otros mecanismos basados en llave pública, en este protocolo se consideran dos niveles de autenticación, en el primero se debe autenticar la fuente del mensaje para efectos de establecer una relación de confianza entre los nodos de la red. Para ello se usa un intercambio de mensajes desafío-respuesta que involucra el esquema de cifrado basado en identidad (IBE: Identity Based Encryption) de Boneh y Franklin [14], para así verificar la autenticidad del suplicante, al mismo tiempo que se lleva a cabo un proceso de acuerdo de llave que será usada para construir el vínculo de confianza entre ambos nodos si la autenticación resulta positiva. En el segundo nivel se requiere autenticar cada mensaje que se recibe de un nodo ya autenticado; para ello se involucra uso de códigos MAC para verificar cada mensaje recibido.

La criptografía basada en identidad (IBC: Identity Based Cryptography), usada a través del esquema de IBE, fue propuesta por Shamir [15] y es una variante de la criptografía de llave pública. Esta tiene como principal característica que las llaves criptográficas se generan a partir de información que identifica a su poseedor, por ejemplo una dirección de correo electrónico. La principal ventaja que ofrece esta técnica es que elimina la necesidad de verificar la autenticidad de las llaves públicas. En cambio, para autenticar

la llave de una entidad solo se requiere realizar el mapeo de su identificador a un elemento del grupo algebraico sobre el cual opera el criptosistema y que corresponderá a su llave pública. La IBC requiere la participación de una entidad de confianza (TA: Trusted Authority), que es la encargada de procesar las llaves públicas, obtenidas mediante el mapeo ya mencionado, para emitir las correspondientes llaves privadas.

Una de las implementaciones más comunes de la IBC es la que hace uso de emparejamientos bilineales sobre puntos de una curva elíptica [14]. Un emparejamiento bilineal es una función racional $\hat{e}$ que mapea un par de elementos de un grupo hacia un elemento de un segundo grupo, tal como se describe en la ecuación 1.

$$\hat{e}: G_1 \times G_1 \rightarrow G_2 \tag{1}$$

El término bilineal denota que la función $\hat{e}$ mantiene la propiedad de bi-linearidad en los términos que se expresan en la ecuación 2, donde P y Q pertenece al grupo G_1 y $\hat{e}(P,Q)$ pertenecen al grupo G_2.

$$\begin{aligned} \hat{e}(aP, bQ) &= \hat{e}(P, bQ)^a \\ &= \hat{e}(aP, Q)^b = \hat{e}(P, Q)^{ab} \end{aligned} \tag{2}$$

Adicionalmente la función $\hat{e}$ debe satisfacer la condición de no degeneración la cual implica que $\hat{e}(P,Q) \neq e_2$ siempre y cuando $P \neq Q$, de otra manera $\hat{e}(P,Q) = e_2$, donde e_2 es el elemento generador del grupo G_2. Para el caso de aplicaciones criptográficas se utiliza como grupo G_1 el grupo aditivo de puntos de una curva elíptica $E(K)$, la cual se define sobre un campo finito $K=G(p^m)$ para algún primo p y un entero m, específicamente el subgrupo de los puntos de torsión r $E[r](K)$, tal como se describe en [16]. Una curva elíptica corresponde al grupo de puntos racionales que tienen correspondencia al lugar geométrico descrito por la ecuación 3 para valores de x y y pertenecientes al campo base K. En lo que corresponde al grupo de puntos de torsión r, éste se define por todos los puntos de $E(K)$ cuyo orden es igual a r, es decir que para un punto S, con $ord(S) = r$, la multiplicación escalar del punto S por r veces equivale al punto al infinito, $[r]S=O$. En lo que respecta al tipo de curva a utilizar, para el caso de emparejamientos se recomiendan curvas supersingulares, y por razones de eficiencia, aquellas definidas sobre campos finitos de característica 2, tal como $K=G(2^m)$ para extensiones del campo con valores de m entre 97 y 459; prefiriendo los valores mas pequeños de m para las WSN [17].

$$E(K): y^2 + ay = x^3 + bx^2 + cx + d, \quad \text{con } a, b, c, d \in K \tag{3}$$

Descripción del protocolo

El protocolo propuesto consta de 6 etapas que van desde la generación de parámetros del sistema, hasta la autenticación de cada mensaje recibido. Estas etapas son: configuración, descubrimiento de nodos, generación del desafío, respuesta, verificación y establecimiento de llave de sesión, y finalmente, la autenticación de mensajes.

Para la definición del protocolo se consideran los siguientes parámetros de dominio: un campo base $K=GF(p^m)$, una curva elíptica $E(K)$, una extensión del campo base $GF(p^{m*k})$ de grado k, así como una función de emparejamiento $\hat{e}$ con parámetro de seguridad k como se describe en la ecuación 4. En cuanto a notación el símbolo $\xleftarrow{\$}$ denota selección aleatoria y el símbolo $a[P]$ denota la multiplicación escalar de a veces P. A continuación se describen a detalle las 6 etapas del protocolo de autenticación, mismas que se detallan más adelante. Una consideración importante es que el administrador de la WSN adoptará el rol de entidad de confianza TA.

$$\hat{e}(P,P) = \langle g \rangle \text{ con } g \in GF(p^{mk}) \tag{4}$$

Configuración. La TA genera los parámetros del sistema así como las llaves de cada nodo sensor de la red. Para ello la TA ejecuta el algoritmo descrito a continuación:

1. Genera dos grupos G_1 y G_2 de orden primo *q*, conforme a la ecuación 4.
2. Selecciona $P \xleftarrow{\$} G_1$
3. Selecciona su llave privada, $s \xleftarrow{\$} \mathbb{Z}_q^*$ y calcula su llave pública por medio de la ecuación 5.

$$P_{pub} = [s]P. \quad (5)$$

4. Define un espacio $\mathcal{L}: \{0,1\}^m$, con *m* acorde al universo de nodos planeado, para generar los identificadores de nodos.
5. Selecciona tres funciones hash criptográficas H_1, H_2 y H_3, tal que $H_1: \{0,1\}^* \rightarrow G_1$, $H_2: G^2 \rightarrow \{0,1\}^n$ y $H_3: \{0,1\}^n \times \{0,1\}^m \rightarrow \{0,1\}^h$, con h=160 o h=163, por ejemplo.
6. Calcula, para cada nodo *i* con identificador, su llave pública según la ecuación 6.

$$Q_i = H_1(ID_i) \text{ con } ID_i \in \mathcal{L} \quad (6)$$

7. Calcula, para cada nodo, su llave privada según la ecuación 7.

$$d_i = [s]Q_i \quad (7)$$

Una vez completado este algoritmo, la TA carga cada nodo con la tripleta (d_i, ID_i, P_{pub}), junto con una lista *TL* vacía de la forma $\{0,1\}^n \times \{0,1\}^m$. Todo el procesamiento de esta etapa se ejecuta en las instalaciones de la TA sin usar recursos de los nodos. En este punto los nodos se despliegan en el área de interés y ejecutan el resto del protocolo cada vez que requieren establecer nuevos enlaces confiables.

Descubrimiento de nodos. Con los nodos desplegados en el área, un primer nodo, ya asociado a la WSN, adopta el rol de nodo autenticador ID_A, mientras que un segundo nodo, que detecta al nodo ID_A, tratará de establecer un enlace confiable con él adoptando el rol de nodo suplicante ID_S; lo anterior se lleva a cabo mediante las siguientes acciones:

1. El nodo ID_S genera un mensaje $m = hello(ID_S, TS)$ y lo envía al nodo ID_A, donde *TS* es una marca de tiempo.
2. El nodo ID_A recibe *m* y valida que la marca de tiempo esté dentro de un umbral *t* para evitar solicitudes muy próximas entre sí por un mismo nodo; si no se observa alguna irregularidad se registra como una solicitud de conexión e inicia el desafío.

Generación del desafío. El nodo ID_A genera el desafío con base en un mensaje cifrado con la llave pública del nodo ID_S, la cual se calcula a partir de su identidad; esto lo hace conforme al siguiente algoritmo:

1. Calcula la llave pública del nodo ID_S por medio de la ecuación 6.
2. Selecciona un entero $r \xleftarrow{\$} \mathbb{Z}_q^*$ y calcula v' por medio de la ecuación 8.

$$v' = H_2\left(\left(\hat{e}\left(Q_{ID_S}, P_{pub}\right)\right)^r\right) \quad (8)$$

3. Selecciona un entero $k \xleftarrow{\$} \{0,1\}^n$ para ser usado como contraseña.
4. Obtiene la contraseña cifrada (u, v) de acuerdo a las ecuaciones 9 y 10.

$$v = k \oplus v' \quad (9)$$

$$u = [r]P \quad (10)$$

5. Envía al nodo ID_S el desafío $Ch = (u, v, ID_A)$

Respuesta. El nodo ID_S descifra el valor de la contraseña *k* utilizando su llave privada d_{ID_S}. Para generar la respuesta se requiere descifrar el desafío y luego utilizar un código MAC H_3, para demostrar que se recuperó el valor *k* correctamente, como se indica a continuación:

1. Recupera el valor de la contraseña por medio de la ecuación 11.

$$\mathrm{k}' = \mathrm{v} \oplus H_2\left(\hat{e}\left(d_{ID_S}, u\right)\right) \quad (11)$$

2. Calcula un token según la ecuación 12 y lo envía como respuesta al nodo ID_A.

$$\tau = H_3(k', ID_S) \quad (12)$$

Verificación y establecimiento de llave de enlace. El nodo ID_A ejecuta la verificación del token τ

para verificar su validez, para ello sustituye $k' = k$ y re-calcula el resultado de la ecuación 12; si la verificación es positiva, entonces se considera al nodo ID_S como autenticado y el valor *k* será adoptado como llave para autenticar las comunicaciones entre los nodos ID_A e ID_S. La llave *k* se almacenará en la lista *TL* de cada nodo.

Autenticación de mensajes. Una vez que dos nodos *i* y *j* se han autenticado entre sí, podrán intercambiar mensajes autenticados por medio de un MAC. Para ello los dos nodos ejecutan las siguientes acciones usando la llave del enlace k_{i-j}:

1. Sea el mensaje *m* el que se va transmitir, el nodo obtiene su código MAC según la ecuación 13 y lo envía con el mensaje.

$$MAC = H_3(k_{i-j}, m) \tag{13}$$

2. El nodo *j* recibe el mensaje y valida la autenticidad del MAC recibido para determinar si lo acepta o no como válido. La validación consiste en re-calcular el valor de la ecuación 13, usando el valor almacenado en su lista TL_j para la llave del enlace, y compararlo contra el MAC recibido. Si existe coincidencia, se cumple la verificación, en caso contrario el mensaje es descartado.

La única condición para establecer la autenticidad de un mensaje es que los nodos involucrados hayan sido autenticados entre sí previamente y con ello exista una llave del enlace acordada entre ambos. En caso contrario, ambos nodos deberán autenticarse como se describe en las etapas 3 a 5 del protocolo propuesto.

Resultados

En esta sección se describe el protocolo propuesto en términos de su efectividad, por medio de una prueba de funcionamiento, y su eficiencia, por medio de una estimación de los costos de transmisión, procesamiento y almacenamiento durante su ejecución, la cual fue obtenida mediante la contabilización de bits transmitidos, primitivas usadas y bits almacenados en memoria.

Efectividad del protocolo

La efectividad del protocolo se describe a continuación para las etapas de autenticación de nodos y autenticación de mensajes.

Efectividad de la autenticación de nodos. Después del descubrimiento de nodos se supone la interacción de dos nodos y , el primero de los cuales asume el rol de autenticador y el segundo el de suplicante. El protocolo prosigue con la generación del desafío por el nodo y éste lo envía al nodo *j* en la forma de la tripleta descrita en la ecuación 14.

$$[u, v, ID_j] = \left[[r]P, k \oplus H_2\left(\left(\hat{e}(Q_j, P_{pub})\right)^r\right), ID_j\right] \tag{14}$$

Una vez que el nodo *j* tiene el desafío, utiliza su llave privada d_j para descifrar *v* y obtener k' en el valor de *k*, aprovechando la bilinealidad del emparejamiento, como se indica en la ecuación 15.

$$\begin{aligned} k' &= v \oplus H_2\left(\hat{e}(d_j, u)\right) \\ &= k \oplus H_2\left(\left(\hat{e}(Q_j, P_{pub})\right)^r\right) \oplus H_2\left(\hat{e}(d_j, [r]P)\right) \\ &= k \oplus H_2\left(\left(\hat{e}(Q_j, [s]P)\right)^r\right) \oplus H_2\left(\hat{e}([s]Q_j, [r]P)\right) \\ &= k \oplus H_2\left(\left(\hat{e}(Q_j, P)\right)^{sr}\right) \oplus H_2\left(\hat{e}(Q_j, P)^{sr}\right) \\ &= k \end{aligned} \tag{15}$$

Con el valor recuperado de *k*, el nodo *j* genera una respuesta al desafío por medio de la ecuación 12, y la envía al nodo *i*. Si la respuesta recibida es correcta, queda demostrado que el nodo *j* conoce su llave privada, que ésta es auténtica y generada por la *TA*, y por tanto dicho nodo pertenece a la WSN.

Efectividad de la autenticación de mensajes. Para establecer la autenticidad de los mensajes intercambiados entre una pareja de nodos *i* - *j*, se considera que ambos nodos han acordado previamente una llave para el enlace k_{i-j}. Esta llave la utiliza el nodo para enviar el mensaje

junto con su código MAC, como prueba de su autenticidad, mientras que el nodo utiliza la copia de dicha llave, para verificar el código recibido. Así pues la efectividad de la autenticación de los mensajes está sujeta al uso de códigos MAC seguros, como el HMAC y NMAC [18], y de funciones hash criptográficas.

Costo del protocolo

Para un protocolo de comunicación orientado a una WSN, el costo de operación es el reflejo del consumo de energía durante la ejecución del mismo, por lo que para obtener su estimado, se requiere considerar el consumo en tres rubros principales: la cantidad de bits transmitida por radio, la cantidad de ciclos de CPU utilizados y la cantidad de bits en memoria requeridos para la manipulación de los mensajes.

Con respecto al primer rubro, el protocolo de autenticación involucra el intercambio de varios mensajes entre los nodos, por lo que se puede estimar su costo en términos de los datos presentados en la tabla 1. En ella se observa que la cantidad de bits transmitidos por el nodo suplicante, durante la autenticación de nodos, es de $32 + m + h$ bits, mientras que el nodo autenticador transmite $n + h + m$ bits. En la misma tabla también se observa la cantidad de bits recibidos, por el suplicante es de $n + h + m$ bits, mientras que para el nodo autenticador es de $32 + m + h$ bits.

Tabla 1 Mensajes transmitidos en el protocolo de autenticación

Etapa	*Mensaje*	*Tx. Aut*	*Rx. Aut*	*Tx. Sup*	*Rx. Sup*
Configuración	-				
Descubrimiento de nodos	$m = hello(ID_s, TS)$		$32 + m$	$32 + m$	
Generación del desafío	$Ch = (u, v, ID_{A'})$	$n + h + m$			$n + h + m$
Respuesta	$\tau = H_3(k', ID_S)$		h	h	
Verificación y establecimiento de llave de enlace					
Autenticación de mensajes	$MAC = H_3(k_{i-j}, m)$	h			h

Haciendo uso de las mediciones de consumo de energía en unidades de radio, reportadas por Peter [19], se hace el siguiente análisis sobre los datos de la tabla 1: se observa una diferencia entre los costos de transmisión y recepción por bit, la cual indica que la transmisión es 1,4 veces más costosa que su recepción, y esta diferencia se transfiere directamente al protocolo de autenticación. Esto le añade una característica de asimetría al protocolo y resulta interesante para prevenir ataques contra el nodo autenticador por parte de nodos que actúen como suplicantes *maliciosos* y que pretendan el agotamiento de la energía de la red. En cuanto al costo derivado del procesamiento, éste es visiblemente mayor comparado con otros protocolos que usan solo criptografía de curva elíptica, la razón de ello es la cantidad de operaciones inmersas en los emparejamientos. En la tabla 2 se describen todas las operaciones involucradas durante las diferentes etapas del protocolo conforme a la siguiente notación: *rnd:* generación de un número aleatorio, *emp:* evaluación de un emparejamiento, *ee:* exponenciación en la extensión de orden k del campo base, *me:* multiplicación escalar de puntos de la curva elíptica, y *hash:* evaluación de una función hash o código MAC. Los costos asociados a la TA se dejan fuera de este análisis que tienen impacto en los recursos de los nodos de la WSN.

Tabla 2 Operaciones criptográficas por nodo ejecutadas por el protocolo de autenticación

Etapa	*Operaciones realizadas en los nodos*	
	Autenticador	*Suplicante*
Configuración		
Descubrimiento de nodos		
Generación del desafío	1 *rnd*, 1 *hash*, 1 *emp*, 1 *ee*, 1 *me*, 1 *xor*	
Respuesta		2 *hash*, 1 *emp*, 1 *xor*
Verificación y establecimiento de llave de enlace	1 *hash*	
Autenticación de mensajes	1 *hash*	1 *hash*

Como se describe en la tabla 2, las principales operaciones que cada nodo ejecuta son un emparejamiento y varias evaluaciones de funciones hash, siendo los emparejamientos los que influirán de manera más significativa en el costo total. Cada emparejamiento, como los involucrados en las ecuaciones 8 y 11, conlleva el cálculo de una cantidad considerable de multiplicaciones escalares, y de multiplicaciones de polinomios sobre el campo base y su extensión de orden *k*. El número preciso de estas operaciones depende del tipo de emparejamiento usado, por ejemplo el emparejamiento *eta-t* propuesto por Barreto [20], el cual es conocido por su eficiencia en su evaluación. Otro factor a considerar para la evaluación del emparejamiento son las técnicas usadas en su implementación, como por ejemplo el uso de coordenadas proyectivas o mixtas, así como el uso de curvas y polinomios reducidos [21]. Los resultados mostrados en la tabla 2 se obtuvieron a partir del análisis de cada una de las etapas del protocolo, y es prácticamente el mismo para ambos nodos, suplicante y autenticador. Esto significa, para este rubro, que existe una simetría en costos para ambos nodos autenticador y suplicante, y señala como una línea de trabajo a futuro el diseño de adecuaciones para generar una condición de asimetría en dichos costos, tal como la observada en el rubro de comunicación por radio. Una última reflexión acerca de la tabla 2, es que aunque los emparejamientos son costosos, éstos solo intervienen durante la fase de autenticación de nodos, la cual representa una fracción muy pequeña del ciclo de vida de un nodo, mientras que la evaluación de códigos MAC es una constante a lo largo de dicho periodo debido, principalmente a la autenticación de mensajes. Esta situación da pie para evaluar la posibilidad de que el costo de los emparejamientos sea intrascendente frente al costo de la autenticación del total de los mensajes recibidos y transmitidos por un nodo durante su vida útil. Esto hace necesario modelar la dinámica del funcionamiento de una WSN para un periodo de observación prolongado. Este modelado dinámico de los costos del protocolo durante la vida de una WSN es otro trabajo a futuro que ayudará a establecer con mayor precisión la viabilidad del protocolo propuesto.

En lo que rubro del almacenamiento corresponde, los espacios de memoria requeridos para la ejecución del protocolo se detallan en la tabla 3, la cual describe la cantidad de memoria en bits requerida y donde l representa la cantidad máxima de enlaces confiables vigentes con otros nodos.

Tabla 3 Necesidades de memoria para la ejecución del protocolo

Etapa	*Memoria en bits usada por nodo*	
	Autenticador	*Suplicante*
Configuración	$2n + m$	
Descubrimiento de nodos		
Generación del desafío	$3n + m$	
Respuesta		$2n + m$
Verificación y establecimiento de llave de enlace	$2m$	
Autenticación de mensajes	$(n + m) * l$	

Se puede observar que la cantidad de bits que se utilizan durante la etapa de autenticación de nodos es de $3*(n + m)$ bits para el nodo autenticador y $2n + m$ bits para el nodo suplicante. Para la etapa de autenticación de mensajes la memoria utilizada puede alcanzar la cantidad de $((n + m) * l_j$ bits para cualquier nodo que ha establecido hasta l enlaces confiables. Estas estimaciones se han obtenido a partir de la observación de variables o piezas de datos usadas en el protocolo, las cuales dejan ver cierto equilibrio entre ambos nodos en lo que a las localidades de memoria se refiere. Por ello se propone la búsqueda de alternativas en el diseño del protocolo para reducir el costo en el nodo autenticador a fin de obtener asimetría en los costos de este rubro.

Finalmente, cabe mencionar, que los resultados descritos en este trabajo son estimaciones sobre el uso de recursos durante la ejecución del protocolo, sin embargo actualmente se está trabajando en las implementaciones de emparejamientos y códigos MAC para efectos de obtener las mediciones experimentales correspondientes.

Conclusiones

En este trabajo se describe el primer protocolo de autenticación con el uso de emparejamientos en ambientes de redes de sensores, el cual ejecuta las tareas de autenticación de nodos y autenticación de mensajes. Este protocolo combina el uso de emparejamientos con el uso de códigos MAC, logrando así aprovechar las ventajas de la criptografía basada en identidad, y acotando el impacto que los emparejamientos pueden tener en la eficiencia de la red.

El uso de primitivas de comunicación de desafío-respuesta, generadas a partir de un esquema de cifrado basado en identidad, hace posible la autenticación de nodos entre sí, verificando la pertenencia a la red y evitando el uso de certificados digitales para el establecimiento de autenticidad de la llave. El mecanismo de autenticación entre nodos propuesto permite el establecimiento de una llave de enlace, la cual es aprovechada posteriormente, junto con códigos MAC, para la autenticación de grandes cantidades de mensajes entre nodos.

Dentro de la estimación de los costos de ejecución del protocolo, particularmente en el rubro de la transmisión de mensajes por radio, se presenta una distribución asimétrica que refleja un mayor costo para el nodo suplicante, lo que otorga una protección ante ataques de abuso de servicio a un nodo de la red que funja como autenticador. Esta asimetría es heredada de los costos de operación de las unidades de radio y se acentúa por las propiedades de los mensajes intercambiados.

Como trabajo a futuro de destaca el análisis dinámico de la eficiencia del protocolo en una WSN durante un período largo de observación reflejando cambios en la topología y así obtener una mejor óptica del impacto del uso de primitivas criptográficas basadas en emparejamientos en estos escenarios. Otro trabajo que se vislumbra es la búsqueda de mejoras al protocolo para lograr asimetría en los costos, tanto de procesamiento, como de almacenamiento, para aumentar el efecto de protección que brinda dicha característica.

Agradecimientos

El primer autor agradece al CONACYT (México), así como al Instituto Politécnico Nacional y al COTEPABE por el apoyo recibido para la realización de este trabajo.

Referencias

1. H. Puccinelli, M. Haenggi. "Wireless sensor networks: applications and challenges of ubiquitous sensing". *IEEE Circuits and Systems*. Vol. 5. 2005. pp. 19-29.
2. Y. Liu. "Information-intensive wireless sensor networks: potential and challenges". *IEEE Communications*. Vol. 44. 2006. pp. 142-174.
3. N. Hashmi, D. Myung, M. Gaynor, S. Moulton. "A sensor-based, web service-enabled, emergency medical response system". *Proc. of USENIX 05*. Anaheim (CA). 2005. pp. 25-29.
4. A. Perring, J. Stankovic, D. Wagner. "Security in wireless sensor networks". *Communications of the ACM*. Vol. 47. 2004. pp. 53-57.
5. P. Kuckertz, A. Junaid, J. Riihijarvi, M. Petri. "Sniper Fire Localization using Wireless Sensor Networks and Genetic Algorithm based Data Fusion". *Proc. IEEE MILCOM 07*. Orlando (Florida). 2007. pp. 1-8.
6. Z. Kolokouris. "Integrity and authencity mechanisms for sensor networks". *International Journal of Computing Research*. Vol. 15. 2007. pp. 57-72.
7. W. Du, J. Deng, Y. S. Han, P. K. Varshney, J. Katz, A. Khalili. "A Pairwise Key Predistribution Scheme for Wireless Sensor Networks". *ACM Transactions on Information and Systems Security*. Vol. 8. 2005. pp. 228-258.
8. G. Li, H. Ling, T. Znati, W. Wu. "A robust on-Demand Path-Key Establishment Framework via Random Key Predistribution for Wireless Sesor Networks". *EURASIP Journal on wireless Communications and Networking*. Vol. 2006. 2006. pp. 1-10.
9. A. S. Wander, N. Gura, H. Eberle, V. Gupta, S. C. Shantz. "Energy Analysis of Public-Key Cryptography for Wireless Sensor Networks". *Proc. 3rd IEEE PERCOM 05*. Kauai (Hawai). 2005. pp. 324-328.
10. L. Uhsadel, A. Poschmann, C. Paar. "Enabling Full-Size Public-Key algorithms on 8-bit Sensor Nodes". *Proc. of 4th European Workshop ESAS*. Cambridge (UK) 2007. pp. 73-86.
11. P. Szczechowiak, L. B. Oliveira, M. Scott, M. Collier, R. Dahab. "NanoECC: Testing the Limits of Elliptic Curve Cryptography in Sensor Networks". *Proc. of European conference on Wireless Sensor Networks (EWSN'08)*. Bologna (Italia). 2008. pp. 305-320.
12. W. Du, R. Wang, P. Ning. "An efficient scheme for authenticating public keys in sensor networks". *Proc. of the 6th ACM international Symposium on Mobile Ad Hoc Networking and Computing*. 2005. Urbana-Champaign (IL). pp. 58-67.
13. L. B. Oliveira, M. Scott, J. Lopez, R. Dahab. "TinyPBC: Pairings for authenticated identity-based non-interactive key distribution in sensor networks". *Proc. of International Conference Networked Sensing Systems INSS2008*. Kanazawa (Japón). 2008. pp. 173-180.
14. D. Boneh, M. Franklin. "Identity based encryption from the Weil pairing". *SIAM Journal of Computing*. Vol. 32. 2003. pp. 586-615.
15. A. Shamir. "Identity-Based Cryptosystems and Signature Schemes". *Proc. of Crypto 84*. Springer LNCS 196. Santa Bárbara (CA). 1985. pp. 47-53.
16. D. Hankerson, A. Menezes, S. Vanstone. *Guide to Elliptic Curve Cryptography*. Springer-Verlag. New York. 2004. pp. 73-86.
17. P. S. L. M. Barreto, H. Y. Kim, B. Lynn, M. Scott. "Efficient Algorithms for Pairing-Based Cryptosystems". *Proc. of Crypto 2002*. Springer. LNCS 2442. Santa Bárbara (CA). 2002. pp. 354-368.
18. H. Krawczyk, M. Bellare, R. Canetti, *HMAC: Keyed-Hashing for Message Authentication, Internet RFC 2104*. 1997.
19. S. Peter, P. Langendörfer, K. Piotrowski. "Public key cryptography empowered smart dust is affordable". *Int. J. of Sensor Networks*. Vol. 3. 2008. pp. 130-143.
20. G. Barreto, S. Héigeartaigh. "Efficient pairing computation on supersingular Abelian varieties". *J. Design, Codes and Cryptography*. Vol 42. 2007. pp. 239-271.
21. J. Beuchat, N. Brisebarre, J. Detrey, E. Okamoto, F. Rodríguez-Henríquez. "A Comparison Between Hardware Accelerators for the Modified Tate Pairing over F2m and F3m". *Pairing 2008 LNCS No. 5209*. Springer. Egham (Reino Unido). 2008. pp. 297-315.