Esquemas de Seguridad Ligeros en Aplicaciones de Redes Inalámbricas de Área Corporal

Ricardo Enrique de la Parra-Aguirre
rdelaparra@tamps.cinvestav.mx
CINVESTAV Tamaulipas
Ciudad Victoria, Tamaulipas, México

Miguel Morales-Sandoval
mmorales@tamps.cinvestav.mx
CINVESTAV Tamaulipas
Ciudad Victoria, Tamaulipas, México

RESUMEN

El sector médico es un área de oportunidad para aplicar tecnologías de la información para monitorizar a los pacientes remotamente, esto es, recolectar los datos de los signos vitales de los pacientes y transferirlos hasta un servidor, para su posterior uso. Esto se logra con la inclusión de tecnologías como redes inalámbricas de área corporal (WBAN), sin embargo, el problema que engloba todo este proceso es la seguridad de los datos; dado que los datos biomédicos recabados son sensibles, se deben mantener privados y protegidos, esto es, garantizar servicios de seguridad como confidencialidad, autenticación, integridad y control de acceso.

PALABRAS CLAVE

wban, seguridad, algoritmos ligeros, servicios de seguridad, sensores

Citar como:
Ricardo Enrique de la Parra-Aguirre and Miguel Morales-Sandoval. 2019. Esquemas de Seguridad Ligeros en Aplicaciones de Redes Inalámbricas de Área Corporal. En *Memorias del Octavo Encuentro de Estudiantes Destacados en el área de Tecnologías de la Información.* CINVESTAV, Ciudad Victoria, TAMPS, MEX, 3 páginas.

1. INTRODUCCIÓN Y PLANTEAMIENTO DEL PROBLEMA

El IoT esta identificada como la siguiente era en las Tecnologías de Información y Comunicación (TICs) donde la computación ocurre en cualquier momento, lugar, y se realiza prácticamente por cualquier "cosa inteligente" [1]. El objetivo principal del IoT es proveer una infraestructura de red con protocolos de comunicación interoperables y software que permita la conexión e incorporación de sensores físicos/virtuales, computadoras, dispositivos inteligentes, automóviles, y objetos como refrigeradores, lavadoras, horno de microondas, comida y medicinas en cualquier momento en cualquier red [2].

Salud, domótica y el sector militar, industrial y agropecuario son áreas de oportunidad relevantes para IoT, donde se requiere un monitoreo continuo y controlado. El inconveniente para estas áreas de aplicación del IoT es la seguridad de los datos; se necesita garantizar que los datos, así como el acceso a los dispositivos sensores deben ser seguros y brindar total integridad de los datos. Diferentes factores hacen que un sistema sea vulnerable, hablando de IoT, desde la arquitectura con la que se desarrolla hasta la forma en la que se utiliza. Las principales amenazas a las que se enfrenta el IoT, tanto a nivel hardware, software y aplicación son: manipulación de la información, ataques maliciosos, espionaje y falsificación [3].

Se ha encontrado en el IoT un área de oportunidad dentro del sector médico; que permita el despliegue de plataformas para el monitoreo de usuarios, recolección de datos y comunicación entre los diferentes usuarios en el entorno médico. Uno de los campos recientes y relevantes son las redes inalámbricas de área corporal (WBANs, por sus siglas en inglés) [4] donde se combinan diversos elementos del IoT para que una red de sensores inalámbricos obtenga los signos vitales de los usuarios. La WBAN se define en IEEE 802.15.6[5] como un estándar de comunicación diseñado para dispositivos de bajo consumo energético y funcionamiento alrededor del cuerpo (humano) y empleado en beneficio de los usuarios. Las WBANs están continuamente recopilando datos fisiológicos para monitorear la condición física de las personas[6].

Aunque la tecnología de WBAN es relativamente incipiente, existe un área de oportunidad en México para la asimilación de esta tecnología y su despliegue en escenarios reales, que coadyuven a combatir los altos niveles de morbilidad en México. Dado que los datos biomédicos tratados en WBANs son sensibles, es decir, son importante en la toma de decisión para la salud del usuario; es esencial que incorpore mecanismos de seguridad eficientes, que sean conscientes de las limitaciones en el poder de cómputo de los nodos sensores. Para garantizar los mecanismos de seguridad [7] como confidencialidad, autenticación, integridad y control de acceso, que son requeridos, sobre la información que se genera, almacena, transmite o procesa [8], es necesario implementar dichos algoritmos ligeros [9] de forma eficiente y segura.

Los principales servicios de seguridad requeridos en una WBAN [4] en las distintas capas de comunicación son:

- **Autenticidad.** Los datos deben ser enviados desde entidades legítimas y ambas partes involucradas son quienes afirman ser.
- **Confidencialidad.** Con el fin de evitar que la información confidencial se revele a personas no autorizadas, los datos deben transmitirse en marcos cifrados.
- **Integridad.** Garantiza que los datos permanecen sin cambios desde su origen hasta el destino. Esto se hace a través de diferentes técnicas como el cifrado.
- **Control de acceso**. Verifica si una entidad solicitando acceso a un recurso tiene los derechos necesarios para hacerlo y garantiza que las entidades solamente accedan a los recursos que necesitan.

La incorporación y uso de tecnología WBAN en e-salud puede tener un impacto significativo en el seguimiento y tratamiento de enfermedades, por ejemplos las derivadas del corazón. Por la

sensibilidad de los datos médicos que maneja, una solución WBAN segura debe considerar desde su diseño el aspecto de la seguridad de los datos, en las diferentes capas de comunicación y procesamiento, esto es, incorporar mecanismos que garanticen los servicios de seguridad requeridos.

2. TRABAJOS RELACIONADO

La revisión de los trabajos relacionados se dividió en tres partes: la primer parte es la revisión de cifradores ligeros más prometedores, la segunda parte son esquemas ligeros de autenticación utilizando criptografía de curva elíptica (ECC, por sus siglas en inglés) o criptografía basada en emparejamientos (PBC, por sus siglas en inglés) y la tercera parte son los prototipos de WBAN propuestos.

2.1. Cifradores ligeros

En los últimos años, un tema relevante dentro del campo de la criptografía han sido los algoritmos ligeros. El propósito de éstos es brindar las mismas propiedades que cualquier cifrador provee, utilizando la menor cantidad posible de los recursos disponibles. Esto tiene varias consideraciones; la primera es que dado el dispositivo en el que es ejecutado un algoritmo ligero, el consumo de los recursos por parte de éste, no debe afectar considerablemente al dispositivo. La segunda consideración es debido a los recursos limitados, no se pueden hacer procesos con tamaños de llaves grandes.

Los principales algoritmos de criptografía de bloques ligera se presentan a continuación:

Tabla 1: Comparación entre algoritmo de cifrado.

Trabajos	Algoritmo	Bloques	Llaves	Rondas	Operaciones
[10, 11]	LEA	128 bits	128, 192, 256 bits	24, 28, 32	ARX
[12, 13]	AES	128 bits	128, 192, 256 bits	10, 12, 14	SPN
[10, 12]	PRESENT	64 bits	80, 128 bits	31	SPN
[10]	CLEFIA	64, 128 bits	128, 192, 256 bits	16	Red Feistel

Los algoritmos seleccionados en la Tabla 1 son los más prometedores y los que se utilizan en algunos trabajos revisados en el estado del arte. Siendo *Present* y *Clefia* estándar *ISO/IEC 29192-2:2012* para cifradores de bloque en criptografía ligera.

2.2. Esquemas ligeros de autenticación

Los algoritmos que utilizan Criptografía de Curva Elíptica (ECC, por sus siglas en inglés) garantizan el servicio de autenticación y debido a las llaves cortas, en comparación con otras variantes, pero equivalente en cuanto al nivel de seguridad, son más eficientes.

Tabla 2: Comparación entre esquemas ligeros de autenticación.

Trabajos	Esquema	ECC/PBC	Autenticación entre nodos	Fases
[7]	Control de acceso	ECC	Sí	Pre-despliegue, Post-despliegue, Registro, Inicio de sesión y Autenticación
[14]	Control de acceso	ECC	Sí	Configuración, Registro y Autenticación e intercambio de llaves.
[10]	Control de acceso	ECC	Sí	Despliegue, Autenticación de nodo y Comunicación segura de datos.
[15]	Control de acceso, firma digital y cifrado	ECC/ABE	Sí	Configuración, Generación de llave, Delegación, Cifrado, descifrado, firma y verificación.

Uno de los aspectos principales a considerar para implementar esquemas criptográficos ligeros en una WBAN, considerando los sensores con recursos limitados, es el consumo de una cantidad reducida de energía en los procesos que se ejecuta.

2.3. Prototipos de WBAN

Los algoritmos ligeros, generalemente se evalúan fuera del contexto de una aplicación particular, como la WBAN. Por ello, es necesario contar con prototipos que permitan evaluar la pertinencia de un algoritmo criptográfico ligero en un entorno de aplicación particular WBAN.

Tabla 3: Comparación entre prototipos propuestos en la literatura.

Trabajos	Arquitectura	Software	ECC/PBC	Algoritmo	Signos vitales	Pruebas
[16]	Imote2	TinyOS	TinyECC	-	-	Velocidad de reloj del Imote2 hasta 416 MHz.
[17]	Microcontrolador de 32 de bits Intel Curie	Arduino, JavaScript	-	LEA	Ritmo cardiaco	Recolección de los signos vitales del paciente y la transmisión a la estación base.

3. PROPUESTA DE INVESTIGACIÓN

Para comprender el tipo de mecanismo de seguridad que implementa una WBAN, primero se necesita conocer la estructura de la comunicación dentro de cada una de estas redes, así como su comunicación con el mundo exterior y con otras WBAN coexistentes. En la Figura 1 se observa una visión general de la estructura de comunicación en WBANs, mostrando que los dispositivos están distribuidos en una red, con la ubicación del dispositivo que actúa como estación base (BS, por sus siglas en inglés) vinculado a una determinada aplicación. Debido a que el cuerpo cambia continuamente la posición, la topología de red no es fija. En la mayoría de los sistemas WBAN, la comunicación que se realiza entre sus componentes se divide en tres capas separadas de la siguiente manera[6]:

- **Capa 1. Recolección de datos:** en esta capa, la interacción de los sensores se limita al cuerpo de un usuario. Las señales de comunicación dentro de la región utilizan una BS, normalmente llamada estación base. Estos pueden ser dispositivos móviles inteligentes como Smartphone o tablets, que actúa como una gateway, para transferir información al siguiente nivel (es decir, gateway que está presente en la capa 2).
- **Capa 2. Comunicación:** esta capa supera la brecha entre la BS y el usuario a través del gateway que se considera una parte importante de la red y pueden ser posicionado de manera que permita casos de emergencia. Esencialmente, la comunicación en este nivel procura conectar la WBAN con otros sistemas o redes para que la información se puede recuperar fácilmente a través de varios medios, como Internet.
- **Capa 3. Aplicación:** en esta capa se realiza el análisis de los datos recolectados y recibidos por parte de WBAN. Por ejemplo, un teléfono inteligente puede convertirse en un puente entre la capa 2 y la 3, o, desde Internet hasta el servidor médico (MS, por sus siglas en inglés) en una aplicación específica. En un entorno médico la base de datos es una parte especialmente importante de la comunicación de esta

capa, ya que contiene el historial médico y el perfil específico del usuario.

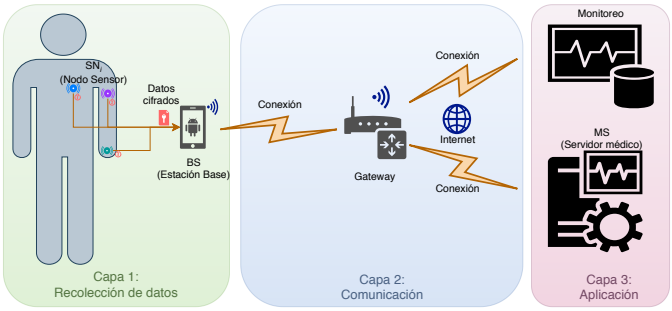

Figura 1: Estructura general de una WBAN segura [6].

La solución propuesta se enfoca en la capa 1: recolección de datos. Ésta contempla la implementación de algoritmos criptográficos ligeros más adecuados en el contexto de la WBAN. La selección de los algoritmos se realiza con una comparación entre los más prometedores.

Todo el esquema criptográfico se desplegará en un prototipo de WBAN, donde se recolecten datos de al menos dos signos vitales de un usuario.

4. PRINCIPALES RESULTADOS Y CONTRIBUCIONES

En esta sección se describen las contribuciones y resultados esperados en este proyecto de investigación. Las contribuciones se presentan a continuación:

- Determinar los algoritmos más viables de criptografía ligera en el estado del arte para usos prácticos en aplicaciones IoT, usando cifrado de siguiente generación.
- Proveer implementaciones y resultados de evaluación de algoritmos altamente recomendables para garantizar servicios de seguridad en aplicaciones de WBAN.
- Proveer un prototipo de WBAN segura para evaluar algoritmos criptográficos de interés en al área de seguridad para IoT.

El resultado esperado es una metodología de diseño de una WBAN segura, en la que se indique cuáles algoritmos criptográficos ligeros son los más adecuados para implementar en este contexto.

5. CONCLUSIONES

Las WBANs tienen un impacto considerable en cuanto a monitorear la condición física de los usuarios. Esto da paso al problema de seguridad sobre los datos que son recolectados. Los datos son sensible, por ende, si sufren algún ataque como espionaje, manipulación, etc., afectan directamente al usuario en observación en caso de tomar alguna decisión respecto a su condición física o, en caso de robo, utilizar los datos para otras aplicaciones.

Al garantizar servicios de seguridad en la recolección de datos de una WBAN se previenen los ataques. Estos servicios de seguridad se garantizan con algoritmos criptográficos y con esto surge un nuevo problema, los algoritmos criptográficos convencionales no son adecuados en el contexto de una wBAN, dado que los recursos de los dispositivos en la red son limitados. La solución es utilizar algoritmos criptográficos ligeros, los cuales son ideales para entornos con dispositivos de bajos recursos computacionales.

Debido a la arquitectura de los nodos sensores, resulta no ser trivial implementar un algoritmo criptográfico ligero en el nodo. Ese es el mayor reto del proyecto. Al terminar el proyecto, se proveerá de una metodología detallada para implementar una WBAN segura utilizando un esquema criptográfico ligero.

REFERENCIAS

[1] A. Sayed and M. Kamal, *Internet of Things Applications, Challenges and Related Future Technologies.* 1 2017.

[2] F. A. Alaba, M. Othman, I. A. T. Hashem, and F. Alotaibi, "Internet of Things security: A survey," *Journal of Network and Computer Applications*, vol. 88, pp. 10–28, 6 2017.

[3] K. R. Siva and R. Venkateswari, "Security Challenges and Solutions for Wireless Body Area Networks," pp. 275–283, Springer, Singapore, 2019.

[4] S. Al-Janabi, I. Al-Shourbaji, M. Shojafar, and S. Shamshirband, "Survey of main challenges (security and privacy) in wireless body area networks for healthcare applications," *Egyptian Informatics Journal*, vol. 18, pp. 113–122, 7 2017.

[5] K. S. Kwak, S. Ullah, and N. Ullah, "An overview of IEEE 802.15.6 standard," in *2010 3rd International Symposium on Applied Sciences in Biomedical and Communication Technologies (ISABEL 2010)*, pp. 1–6, IEEE, 11 2010.

[6] Z. Shihong, X. Yanhong, W. Honggang, L. Zhouzhou, C. Shanzhi, and H. Bo, "A Survey on Secure Wireless Body Area Networks," *Security and Communication Networks*, vol. 2017, p. 9, 2017.

[7] S. Chatterjee, A. K. Das, and J. K. Sing, "A novel and efficient user access control scheme for wireless body area sensor networks," *Journal of King Saud University - Computer and Information Sciences*, vol. 26, pp. 181–201, 7 2014.

[8] M. Masdari and S. Ahmadzadeh, "Comprehensive analysis of the authentication methods in wireless body area networks," *Security and Communication Networks*, vol. 9, pp. 4777–4803, 11 2016.

[9] A. Shah and M. Engineer, "A Survey of Lightweight Cryptographic Algorithms for IoT-Based Applications: Proceedings of ICSICCS-2018," pp. 283–293, 1 2019.

[10] I. Jawaid, A. Noor ul, I. Arif, and D. Nizamud, "Efficient Key Agreement and Nodes Authentication Scheme for Body Sensor Networks," *International Journal of Advanced Computer Science and Applications*, vol. 8, no. 7, p. 8, 2017.

[11] J. Choi and Y. Kim, "An improved LEA block encryption algorithm to prevent side-channel attack in the IoT system," in *2016 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA)*, pp. 1–4, IEEE, 12 2016.

[12] G. Hatzivasilis, K. Fysarakis, I. Papaefstathiou, and H. Manifavas, *A review of lightweight block ciphers*, vol. 8. 4 2017.

[13] A. Altigani, M. Elsadig, and B. Barry, *Evaluating AES Performance Using NIST Recommended Block Cipher Modes of Operation.* 5 2015.

[14] J. Zhang, N. Xue, and X. Huang, "A Secure System For Pervasive Social Network-Based Healthcare," *IEEE Access*, vol. 4, pp. 9239–9250, 2016.

[15] J. Hong, B. Liu, Q. Sun, and F. Li, "A combined public-key scheme in the case of attribute-based for wireless body area networks," *Wireless Networks*, vol. 25, pp. 845–859, 2 2019.

[16] D. Baehr, S. McKinney, A. Quirk, and K. Harfoush, "On the practicality of elliptic curve cryptography for medical sensor networks," in *2014 11th Annual High Capacity Optical Networks and Emerging/Enabling Technologies (Photonics for Energy)*, pp. 41–45, 2014.

[17] A. Z. Alshamsi and E. S. Barka, "Implementation of energy efficient/lightweight encryption algorithm for wireless body area networks," in *2017 International Conference on Informatics, Health & Technology (ICIHT)*, pp. 1–7, IEEE, 2 2017.

"Este artículo de divulgación se refiere al trabajo de investigación que se realiza en el marco del proyecto 281565 del Fondo de Investigación para la Educación SEP-CONACYT, bajo la dirección del Dr. Miguel Morales Sandoval."