Esquemas de seguridad ligeros en aplicaciones de redes inalámbricas de área corporal

Ricardo de la Parra,* Miguel Morales*

*{rdelaparra, mmorales}@tamps.cinvestav.mx

Contexto

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.

Contribuciones

- 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 representativas de IoT.
- Proveer un prototipo experimental de WBAN segura para evaluar algoritmos criptográficos de interés en al área de seguridad para IoT.

Antecedentes

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 en IoT son las redes inalámbricas de área corporal (WBAN)[1]. Las WBANs se definen en IEEE 802.15.6[2] 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. Dado que estos dispositivos son pequeños, los recursos computacionales son limitados. Existe un campo de estudio de "criptografía ligera" que estudia algoritmos criptográficos que puedan usarse para garantizar servicios de seguridad en entornos de cómputo restringido [3].

Motivación

En México, hasta el 31 de octubre de 2018, el 88.6 % de las defunciones se debieron a enfermedades y problemas relacionados con la salud. En una WBAN, los nodos sensores recolectan signos vitales de los usuarios, que podrían servir para detectar anomalías en su comportamiento e informar oportunamente cuando el usuario necesita ser atendido.

Rango	Total	Hombres	Mujeres
1	Enfermedades del corazón 141 619	Enfermedades del corazón 75 256	Enfermedades del corazón 66 337
2	Diabetes mellitus 106 525	Diabetes mellitus 52 309	Diabetes mellitus 54 216
3	Tumores malignos 84 142	Tumores malignos 41 088	Tumores malignos 43 053

Figura: Principales causas de muerte en México durante 2017.

Planteamiento del problema

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 esencial que una WBAN incorpore mecanismos de seguridad eficientes, que sean conscientes de las limitaciones en el poder de cómputo de los nodos sensores, debido a la tendencia de integración de dispositivos cada vez más pequeños. Para proporcionar los mecanismos de seguridad [4] y garantizar servicios de seguridad requeridos como: confidencialidad, autenticación, integridad y control de acceso sobre la información que se genera, almacena, transmite o procesa [5], es necesario implementar algoritmos ligeros [6] de forma eficiente y segura.

Preguntas de investigación

1. ¿Cuáles son los algoritmos de criptografía ligera más recomendables para garantizar servicios de confidencialidad, integridad, autenticación y control de acceso en aplicaciones reales de e-salud usando WBANs?
2. ¿Qué costo computacional e impacto asociado tienen los algoritmos de criptografía ligera, cuando se evalúan en aplicaciones representativas de IoT como e-salud mediante WBANs, y cuáles son las métricas de mayor interés?
3. ¿Desde el punto de vista de la implementación, cuáles son los problemas abiertos en cuanto a diseño e implementación de algoritmos de criptografía ligera para aplicaciones de e-salud en el contexto de WBAN?

Hipótesis

Es posible eficientizar el consumo de energía de los nodos sensores corporales de una WBAN segura, garantizando servicios de confidencialidad, integridad, autenticación y control de acceso, mediante el uso de algoritmos de criptografía ligera en un entorno real de e-salud en aplicaciones de IoT.

Objetivo general

Definir una metodología de diseño de WBAN segura, que considere e incorpore mecanismos de criptografía ligera para garantizar servicios de confidencialidad, integridad, autenticación y control de acceso en la capa de recolección de datos del modelo WBAN, haciendo eficiente el consumo de energía de los nodos sensores con un bajo sobrecosto de los recursos computacionales proporcionados.

Objetivos específicos

1. Determinar los algoritmos de criptografía ligera más adecuados para proveer un entorno de aplicación WBAN segura y garantizar los servicios de confidencialidad, integridad, autenticación y control de acceso.
2. Determinar el impacto de la provisión de servicios de seguridad mediante algoritmos de criptografía ligera en aplicaciones de WBAN segura representativas en el contexto e-salud de IoT.
3. Definir un flujo de diseño de WBAN segura, tomando en cuenta el modelo genérico y las tecnologías más adecuadas para su despliegue.

Solución propuesta

La solución propuesta se centra en garantizar servicios de seguridad como: confidencialidad, autenticación, integridad y control de acceso en la capa 1 de recolección de datos de la estructura de una WBAN segura. Los procesos que se proponen realizar para asegurar la WBAN son los siguientes:

- Evaluar y seleccionar cifradores ligeros con mejor rendimiento en las pruebas.
- Diseñar e implementar una red inalámbrica de sensores corporales para recolectar los datos de los usuarios.
- Cifrar los datos recolectados mediante los nodos sensores, utilizando el cifrador ligero más adecuado en ese contexto.
- Utilizar un esquema de autenticación de nodos sensores cuando se comunican con la estación base utilizando cifrado de curva elíptica.

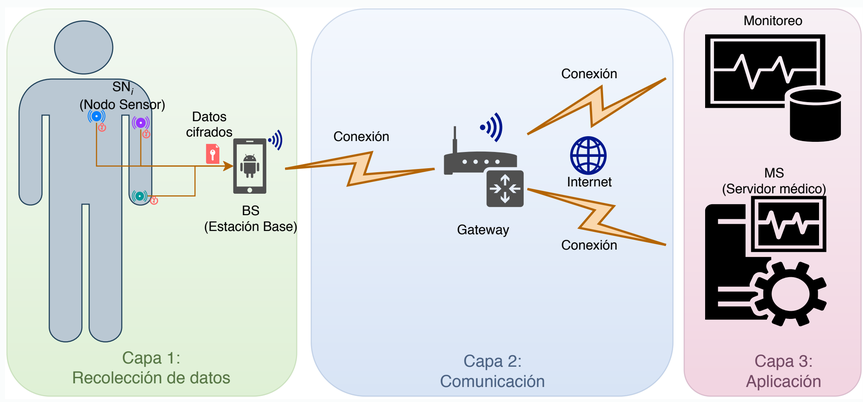

Figura: Estructura general de una WBAN segura, dividida en las tres capas que la conforman.

Referencias

[1] 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.

[2] 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.

[3] S. Singh, P. K. Sharma, S. Y. Moon, and J. H. Park, "Advanced lightweight encryption algorithms for IoT devices: survey, challenges and solutions," *Journal of Ambient Intelligence and Humanized Computing*, 2017.

[4] 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.

[5] 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.

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

"Este proyecto corresponde a una tesis de maestría 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."

Cinvestav Tamaulipas