UNIVERSIDAD DE CHILE
FACULTAD DE CIENCIAS FÍSICAS Y MATEMÁTICAS
DEPARTAMENTO DE INGENIERÍA ELÉCTRICA

PROPUESTA DE ESQUEMAS CRIPTOGRÁFICOS Y DE TRANSMISIÓN PARA ARQUITECTURAS LPWAN EN EHEALTH

TESIS PARA OPTAR AL GRADO DE MAGISTER EN CIENCIAS DE LA INGENIERÍA, MENCIÓN ELÉCTRICA

NICOLÁS ALBERTO RUMINOT AHUMADA

PROFESOR GUÍA:
CLAUDIO ESTEVEZ MONTERO

PROFESOR CO-GUÍA:
SAMUEL MONTEJO SÁNCHEZ

MIEMBROS DE LA COMISIÓN:
HECTOR KASCHEL CÁRCAMO
CESAR AZURDIA MEZA

Este trabajo ha sido parcialmente financiado por Proyecto ANID FONDECYT Iniciación No. 11200659 y ANID FONDECYT Regular No. 1241977.

SANTIAGO DE CHILE
2024

RESUMEN DE LA TESIS PARA OPTAR AL GRADO DE
MAGÍSTER EN CIENCIAS DE LA INGENIERÍA,
MENCIÓN ELÉCTRICA
POR: NICOLÁS ALBERTO RUMINOT AHUMADA
FECHA: 2024
PROF. GUÍA: CLAUDIO ESTEVEZ MONTERO
PROF. CO-GUÍA: SAMUEL MONTEJO SÁNCHEZ

PROPUESTA DE ESQUEMAS CRIPTOGRÁFICOS Y DE TRANSMISIÓN PARA ARQUITECTURAS LPWAN EN EHEALTH

El desarrollo exponencial de las tecnologías del Internet de las Cosas (IoT) no tiene precedentes. Actualmente, estas tecnologías están integradas en casi todas las áreas de la ciencia y la vida cotidiana, destacando en sectores críticos como el área de la salud. En estos entornos, los dispositivos IoT, generalmente con recursos computacionales muy limitados, procesan información altamente sensible, incluyendo signos vitales e información médica. Por lo tanto, es imperativo estudiar medidas que garanticen la fiabilidad de las comunicaciones y la seguridad de la información en estas aplicaciones.

Se implementaron y evaluaron algoritmos criptográficos como Ascon-128a para criptografía simétrica y secp256r1 para criptografía asimétrica, utilizando microcontroladores de bajo consumo, como el ESP32 y ATMEGA328P. Estas pruebas experimentales fueron complementadas con simulaciones detalladas para medir su rendimiento, consumo de memoria y resistencia a ataques de canal lateral. Además, se evaluaron esquemas de transmisión en redes LPWAN mediante simulaciones Monte Carlo, con el fin de garantizar la confiabilidad de las comunicaciones en entornos eHealth. Se midió la probabilidad de interrupción bajo diversas condiciones de canal, utilizando técnicas de redundancia y codificación para optimizar la transmisión de datos.

Los resultados mostraron que la implementación combinada de Ascon-128a y secp256r1 es viable para proteger y encadenar la información en dispositivos de recursos limitados, garantizando la confiabilidad, la integridad y la autenticidad de los datos transmitidos. Este enfoque se presenta como una solución robusta y realista para mitigar los riesgos inherentes a la seguridad en dispositivos IoT de recursos limitados. Los esquemas de transmisión con codificación lograron una cobertura de hasta 16,1 km, duplicando el alcance en comparación con transmisiones sin redundancia y superando al mejor esquema de replicas idénticas por 1,9 km. Además, se abordaron las vulnerabilidades inherentes a los dispositivos IoMT, proponiendo el uso de blockchain para mitigar los principales vectores de ataque.

"Salgo a pasear por dentro de mí,
Veo paisajes que de un libro,
De memoria me aprendí"
Roberto Iniesta

Agradecimientos

Últimamente, he estado reflexionando sobre los privilegios en la vida, lo que es justo y lo que no, el mérito y lo merecido. A veces pienso en cómo cuantificar la suerte de las personas: la suerte al nacer, las habilidades innatas y las adquiridas. Sin duda, la naturaleza de cada individuo representa una ventaja o desventaja, así como las condiciones externas que moldean y refinan nuestro carácter y habilidades. Es fascinante la variedad de suertes entre las personas. Sin embargo, puedo afirmar sin lugar a dudas que mi mayor fortuna proviene de mi familia, amigos y profesores; ellos son mi mayor privilegio.

A todos ustedes, gracias.

"La vida de cada hombre es un camino hacia sí mismo,
el intento de un camino,
el esbozo de un sendero."
Hermann Hesse

Tabla de Contenido

Índice de Tablas

Índice de Figuras

Acrónimos

3GPP 3rd Generation Partnership Project

AD Associated Data

AES Advanced Encryption Standard

DoS Denial Of Service

ECDH Elliptic-curve Diffie–Hellman

ECDSA Elliptic Curve Digital Signature Algorithm

ECC Elliptic-curve Cryptography

FI Fault Injection

GDPR General Data Protection Regulation

HIPAA Health Insurance Portability and Accountability Act

IoMT Internet of Medical Things

IoT Internet of Things

LPWAN Low Power Wide Area Network

LWC Lightweight Cryptography

MAC Message Authentication Code

NB NarrowBand

QoE Quality of Experience

QoS Quality of Service

RTT Round Trip Time

SINR Signal-to-Interference-plus-Noise Ratio

SNR Signal to Noise Ratio

SPN Substitution-Permutation Network

WPAN Wireless Personal Area Network

WSN Wireless Sensor Network

Capítulo 1

Introducción

1.1. Motivación

El Internet de las Cosas (IoT) representa una tecnología innovadora que actualmente lidera la expansión de conexiones a Internet. Según un informe reciente de Statista, se espera que este número continúe en aumento, proyectando alcanzar 38 mil millones de conexiones IoT para el año 2030 [1]. La versatilidad operativa del IoT lo ha integrado en diversas industrias y campos de actividad humana, incluyendo sectores críticos como la infraestructura eléctrica y la atención médica. En estos ámbitos, la disponibilidad y la seguridad de la información son de suma importancia.

Esta tesis aborda desafíos de seguridad derivados del uso de tecnologías LPWAN y dispositivos IoMT en eHealth, proponiendo un esquema criptográfico que garantice la seguridad y esquemas de comunicación que garantizan la confiabilidad. Se realiza un análisis detallado del enlace de bajada, ya que su correcto funcionamiento es fundamental para procesos críticos como la actualización de firmware. Esta tarea es especialmente relevante en los dispositivos IoMT, muchos de los cuales carecen de mecanismos adecuados para actualizar su firmware, lo que los hace vulnerables a posibles ataques y compromete su seguridad [2]. Se adopta un enfoque clásico en seguridad de la información, conocido como la "triada de la seguridad información", que busca salvaguardar la confidencialidad, la integridad y la disponibilidad de los datos, además de garantizar el no repudio y la privacidad [3]. Asimismo, se evalúa la viabilidad de esquemas de comunicación que aseguren una transmisión confiable y sin errores, y se seleccionan algoritmos criptográficos adecuados para su implementación en dispositivos IoMT con recursos limitados.

La implementación de cifrados ligeros y tecnología blockchain ofrece soluciones robustas a los desafíos de seguridad e interoperabilidad en sistemas eHealth [4]. Particularmente, blockchain ha demostrado ser una herramienta efectiva en la actualización de firmware, proporcionando un registro inmutable que garantiza la integridad de las actualizaciones y previene modificaciones no autorizadas [5]. Por otro lado, los cifrados ligeros son esenciales para los dispositivos IoMT, que a menudo cuentan con recursos limitados en términos de procesamiento y energía. Estos cifrados permiten proteger la información sin imponer una carga significativa en los dispositivos, asegurando que la comunicación sea segura y eficiente [6, 7].

Por otro lado, la tecnología blockchain proporciona un registro inmutable y distribuido de todas las transacciones, lo que incrementa la transparencia y la trazabilidad de los datos. Esta característica es especialmente beneficiosa en el ámbito de la atención médica, donde la integridad y autenticidad de los datos son fundamentales [4]. Blockchain utiliza técnicas criptográficas avanzadas para garantizar que los datos no sean alterados sin autorización, y su naturaleza descentralizada facilita la interoperabilidad, permitiendo la integración de datos provenientes de múltiples fuentes y mejorando la coordinación y continuidad de la atención médica. Además, los contratos inteligentes en blockchain pueden gestionar permisos de acceso, otorgando a los pacientes un mayor control sobre sus datos personales y garantizando que solo las partes autorizadas puedan acceder a su información.

El estudio de esquemas de comunicación adecuados es igualmente crucial. La viabilidad de esquemas que aseguren una transmisión confiable y sin errores debe ser analizada teórica y analíticamente, considerando las limitaciones y requisitos específicos de los dispositivos IoMT. La combinación de cifrados ligeros, tecnología blockchain y esquemas de comunicación optimizados puede proporcionar una solución integral a los desafíos de seguridad y eficiencia en eHealth [8].

En resumen, esta tesis propone esquemas de transmisión y criptográficos para sistemas eHealth, abordando los recursos disponibles en los dispositivos, la confiabilidad de la transmisión y la seguridad de la información en el área de la salud. La integración de criptografía ligera y blockchain promete mejorar significativamente la seguridad y la interoperabilidad en estos sistemas, proporcionando una base sólida para un sistema de salud más seguro y eficiente.

1.2. Planteamiento del Problema e Hipótesis

1.2.1. Planteamiento del Problema

En el contexto de la atención médica, la adopción de tecnologías del Internet de las Cosas Médicas (IoMT) ha facilitado la recolección y monitoreo de datos de manera más eficiente y en tiempo real, mejorando significativamente la calidad de la atención y la gestión de los pacientes. Sin embargo, esta integración masiva de dispositivos conectados plantea importantes desafíos en términos de seguridad y privacidad. Los dispositivos IoMT suelen operar con recursos limitados y están distribuidos en redes amplias y heterogéneas, lo que dificulta la implementación de actualizaciones cuando se descubren nuevas vulnerabilidades. Esta falta de métodos adecuados para actualizar dichos dispositivos aumenta su exposición a posibles ataques y fallos de seguridad, siendo este uno de los principales problemas que afectan la confiabilidad y seguridad de los sistemas IoMT.

Además, la interoperabilidad entre diferentes sistemas de salud continúa siendo un desafío crucial. La falta de estándares unificados y la dependencia de infraestructuras centralizadas pueden generar inconsistencias en los datos, provocar retrasos en la comunicación y dificultar la gestión y acceso a la información. Abordar estos problemas es fundamental para mejorar la seguridad, el intercambio de información y la eficiencia de los dispositivos IoMT en entornos de atención médica.

En el ámbito de eHealth, la seguridad de la información no es solo una cuestión técnica, sino una necesidad vital. La confidencialidad, integridad y disponibilidad de los datos médicos pueden ser literalmente una cuestión de vida o muerte. Cualquier brecha en la seguridad puede comprometer la privacidad del paciente, causar errores en el diagnóstico o tratamiento, y poner en riesgo la seguridad y bienestar de los pacientes.

A pesar de los avances en la criptografía y las tecnologías de red, la implementación efectiva de estas soluciones en entornos eHealth sigue siendo limitada. Es fundamental que los esquemas de comunicación no solo sean seguros, sino también altamente confiables, garantizando que los datos se transmitan de manera precisa y sin errores. El estudio de la confiabilidad del canal en el enlace de bajada es clave en este contexto, ya que muchas aplicaciones IoMT, como las actualizaciones de firmware, dependen de este enlace para garantizar la seguridad y la correcta operación de los dispositivos. La necesidad de garantizar la confidencialidad, integridad, disponibilidad, no repudio y privacidad de la información de salud no se puede subestimar, ya que cualquier brecha podría tener consecuencias graves para la seguridad de los pacientes y la eficiencia del sistema de salud.

1.2.2. Hipótesis

Establecemos la hipótesis del trabajo de la siguiente manera:

- La integración de tecnologías avanzadas como cifrados ligeros, blockchain y esquemas de comunicación codificados mejorará significativamente la seguridad, la interoperabilidad y la confiabilidad de los sistemas eHealth.

1.3. Objetivos

Los objetivos del trabajo se resumen a continuación:

- **Objetivo general:** Desarrollar y validar esquemas de comunicación seguros, confiables e implementables en dispositivos LPWAN usados en eHealth, mejorando la interoperabilidad y la confiabilidad en la transmisión de los datos médicos, con una seguridad garantizada de 128 bits.
- **Objetivos específicos:**
  - Evaluar y analizar las diferentes arquitecturas propuestas para abordar los desafíos de eHealth.
  - Comparar la efectividad de los cifrados ligeros en la protección de datos en dispositivos IoMT, analizando su impacto en el rendimiento, el nivel de seguridad que otorgan y el uso de recursos computacionales que requieren.
  - Analizar y diseñar distintos esquemas de transmisión que garanticen la confiabilidad de la comunicación, comparándolos con esquemas tradicionales en base a la probabilidad de interrupción, asegurando que dicha probabilidad se mantenga por

debajo de un umbral preestablecido igual a 0.1.

- Implementar una solución basada en blockchain que proporcione un registro inmutable y distribuido de las transacciones médicas, mejorando la integridad, autenticidad y transparencia de los datos en sistemas eHealth.

- Evaluar la implementación de los esquemas propuestos en un entorno simulado bajo distintos modelos de canal comparando su efectividad en términos de seguridad y confiabilidad.

1.4. Contribuciones

La principal contribución de esta investigación es la propuesta y el análisis de esquemas de comunicación basados en blockchain, diseñados específicamente para ser implementados en dispositivos de recursos limitados en una arquitectura eHealth. Estos esquemas se analizan en términos de los recursos necesarios y la probabilidad de interrupción, logrando mejorar la cobertura en comparación con los esquemas tradicionales de repeticiones idénticas [8]. Además, se aborda el problema de la seguridad en las comunicaciones, respaldado por una exhaustiva revisión bibliográfica sobre las técnicas criptográficas más adecuadas para dispositivos con recursos limitados. A partir de esta revisión, se realiza una comparación práctica de los recursos requeridos por diferentes algoritmos de cifrado, y se propone un esquema de seguridad que cumple con el nivel 2 de seguridad establecido por la norma IEEE 802.15.6 implementable en dichos dispositivos. Por último, se estudia una amplia gama de vulnerabilidades presentes en dispositivos de recursos limitados, proporcionando un enfoque integral para su mitigación [9].

1.5. Estructura de la Tesis

La estructura de esta tesis es la siguiente: En el Capítulo 2 se presenta la metodología utilizada para su desarrollo. El Capítulo 3, se revisan brevemente algunos conceptos necesarios para entender el resto de la investigación. En el Capítulo 4, presentamos el modelo del sistema y los esquemas propuestos basados en las revisiones bibliográficas realizadas. En el Capítulo 5, se discuten y analizan los resultados obtenidos, comparándolos con otros resultados de la literatura. Finalmente, en el Capítulo 6, se presentan las conclusiones y el trabajo futuro.

Capítulo 2

Metodología

En esta sección se describe la metodología empleada para evaluar el rendimiento de los esquemas criptográficos y de transmisión propuestos en dispositivos IoT de recursos limitados. La evaluación se llevó a cabo mediante simulaciones detalladas y pruebas en hardware real para garantizar que los resultados sean representativos de escenarios prácticos. La metodología se centra en la comparación de algoritmos criptográficos y su implementación en plataformas de bajo consumo, así como en la evaluación de los recursos necesarios y la efectividad de los esquemas propuestos.

2.1. Revisión Bibliográfica y Selección de Algoritmos Criptográficos

Para garantizar el cumplimiento de los objetivos del estudio, se realizó una exhaustiva revisión bibliográfica, enfocada en identificar los esquemas criptográficos y de comunicación más adecuados para ser implementados en dispositivos de recursos limitados dentro de un contexto de arquitectura eHealth. La revisión incluyó tanto algoritmos simétricos como asimétricos, así como funciones hash y esquemas de autenticación. Los algoritmos se seleccionaron basándose en su rendimiento demostrado en la literatura y su adecuación a dispositivos con limitaciones de memoria y procesamiento.

Entre los algoritmos evaluados se encuentran AES-128 y Ascon-128a para criptografía simétrica, Curve25519 y secp256r1 para criptografía asimétrica, y BLAKE2s y Ascon-Hash para funciones hash. Cada uno de estos algoritmos fue revisado en términos de seguridad, eficiencia computacional y requerimientos de recursos, especialmente en plataformas de bajo consumo energético como los microcontroladores ESP32 y ATMEGA328P.

2.2. Evaluación Comparativa de Esquemas de Comunicación

Además de la criptografía, la investigación incluyó un análisis detallado de esquemas de transmisión en redes LPWAN, especialmente dentro del ámbito de eHealth. Se evaluaron

varios esquemas de transmisión que incorporan técnicas de redundancia y codificación para mejorar la confiabilidad y la cobertura en entornos de comunicaciones inalámbricas de largo alcance.

La comparación entre los esquemas de transmisión se realizó utilizando simulaciones Monte Carlo, permitiendo una evaluación detallada de la probabilidad de interrupción de la información en diferentes escenarios de canal y condiciones de transmisión. Los resultados obtenidos se utilizaron para seleccionar los esquemas de transmisión más robustos en términos de confiabilidad y eficiencia energética.

2.3. Implementación y Pruebas en Hardware

Una vez seleccionados los algoritmos criptográficos y los esquemas de transmisión, se procedió a la implementación de estos algoritmos en las plataformas ESP32 y ATMEGA328P. Los parámetros de simulación, como carga útil y firma, se basaron en el tamaño de la salida generada por los algoritmos criptográficos seleccionados, mientras que los demás parámetros siguieron los valores típicos de NB-IoT para asegurar la relevancia y realismo de los resultados. Las simulaciones se llevaron a cabo en un procesador Ryzen 7 5800H de 3.2 GHz utilizando técnicas de Monte Carlo para validar los modelos analíticos.

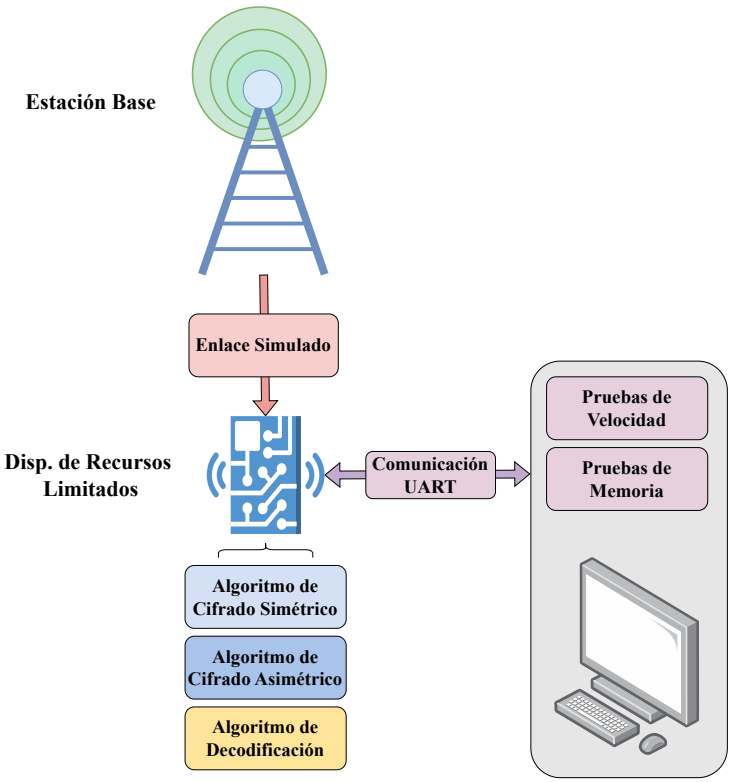


Figura 2.1: Esquema detallado de configuración experimental utilizado para la implementación y evaluación de los algoritmos en plataformas de bajo consumo. El esquema incluye los componentes principales: dispositivos de recursos limitados, algoritmos implementados y enlace simulado para pruebas de confiabilidad.

Se realizaron pruebas exhaustivas para medir el uso de memoria (RAM y Flash), los ciclos de reloj necesarios para las operaciones criptográficas, y el rendimiento general de los esquemas de transmisión en condiciones de baja potencia. Durante estas pruebas, se midieron los recursos necesarios para la implementación de los algoritmos criptográficos y los esquemas de codificación, lo que incluyó memoria (Flash y RAM) y ciclos de reloj. La configuración experimental se puede observar en la Figura 2.1. Adicionalmente, las implementaciones se evaluaron bajo escenarios de uso realista, analizando también su resistencia a ataques de canal lateral y otros vectores de ataque comunes en entornos de IoT.

2.4. Validación de Resultados

La validación de los modelos analíticos se realizó mediante simulaciones de Monte Carlo, logrando una coincidencia con un nivel de confianza del 95 %. Además, las implementaciones de algoritmos criptográficos en hardware se llevaron a cabo en dos microcontroladores: el ESP32 WROOM-32D y el ATMEGA328P, para medir su rendimiento. Las pruebas incluyeron la evaluación de ciclos de reloj y uso de memoria durante la ejecución de operaciones de cifrado, descifrado, intercambio de llaves y calculo del valor hash. Adicionalmente, los resultados de las mediciones se compararon con los reportados en la literatura, mostrando una consistencia con los hallazgos. Este proceso permitió verificar la viabilidad de los algoritmos y esquemas seleccionados, asegurando que cumplían con los estrictos requisitos de seguridad y eficiencia necesarios para su implementación en arquitecturas eHealth.

Finalmente, se realizó un análisis de seguridad para evaluar la resistencia de los algoritmos criptográficos frente a diversos vectores de ataque, tales como ataques de fuerza bruta, ataques de canal lateral y ataques criptográficos avanzados. De este modo, se establece una base sólida para la selección y validación de soluciones criptográficas y de comunicación en dispositivos de recursos limitados, garantizando tanto la seguridad como la eficiencia operativa en entornos críticos como el eHealth.

Capítulo 3

Marco Teórico

En este capítulo se presentan las definiciones necesarias para comprender el resto de la investigación. Se abordan temas fundamentales como eHealth, incluyendo sus arquitecturas, dispositivos y los esquemas de transmisión y confiabilidad. Además, se exploran conceptos relacionados con blockchain, criptografía y las vulnerabilidades asociadas a eHealth. También se incluyen las normas y regulaciones pertinentes, como IEEE 802.15.6 [10], la Ley de Portabilidad y Responsabilidad del Seguro de Salud (HIPAA, por sus siglas en inglés) [11], que regula la protección de la información médica en Estados Unidos; el Reglamento General de Protección de Datos (GDPR) de la Unión Europea [12], y la Ley de Protección de Datos Personales en Chile [13], con el fin de establecer el marco normativo y de seguridad que deben cumplir los sistemas de salud electrónicos.

Cada uno de estos conceptos es analizado en profundidad mediante una revisión bibliográfica exhaustiva, incorporando referencias y discusiones relevantes. Esta revisión bibliográfica permite contextualizar cada tema dentro del marco teórico existente, proporcionando una base sólida para la investigación. Así, se garantiza que las definiciones y conceptos presentados estén respaldados por la literatura científica actual, facilitando una comprensión integral y actualizada de los desafíos y soluciones en el ámbito de eHealth.

3.1. eHealth

eHealth, también conocida como salud electrónica, es un término amplio que se refiere al uso de las tecnologías de la información y las comunicaciones en la atención médica. Este concepto abarca una amplia variedad de subdominios de la salud digital, como registros electrónicos de salud, telesalud, sistemas informáticos de salud y big data.

La Organización Mundial de la Salud (OMS) define eHealth como el uso rentable y seguro de las tecnologías de la información y la comunicación para satisfacer las necesidades de los ciudadanos, pacientes, profesionales y proveedores de atención médica [14]. Por otro lado, el Journal of Medical Internet Research define eHealth como un campo emergente en la intersección de la informática médica, la salud pública y las empresas, que se refiere a los servicios de salud e información entregada o mejorada a través de Internet y las tecnologías relacionadas [15].

Dependiendo de cómo se elija definirlo, eHealth puede abarcar una amplia variedad de subdominios de salud digital, tales como registros electrónicos de salud (EHR), registros médicos electrónicos (EMR), telesalud y telemedicina, sistemas informáticos de salud, datos

de TI de salud del consumidor, asistencia sanitaria virtual, salud móvil (mHealth), y sistemas de big data utilizados en salud digital.

En el Internet de las Cosas (IoT), los dispositivos recopilan y comparten información directamente entre sí y con la nube, permitiendo recoger, registrar y analizar nuevos flujos de datos de forma más rápida y precisa. IoT representa un avance significativo en el campo de la salud electrónica, donde ya se aplica para mejorar la calidad de la atención, aumentar el acceso y, lo más importante, reducir los costos. Sin embargo, este crecimiento en la circulación de información plantea numerosos desafíos. Toda la información generada y procesada en estos subdominios de la salud digital debe cumplir con las normativas o leyes específicas del país o región de origen. En [4] se aborda este desafío a través de un enfoque basado en blockchain para sistemas IoMT.

3.1.1. Internet de las Cosas Médicas

El Internet de las Cosas Médicas (IoMT, Internet of Medical Things) se define como una aplicación de la Internet de las Cosas (IoT, Internet of Things) que permite el uso de dispositivos médicos conectados para detectar datos fisiológicos, almacenar información médica y/o registros, y proporcionar servicios de atención médica utilizando redes de sensores y actuadores y la Internet [16]. Los dispositivos IoMT abarcan desde dispositivos y equipos a gran escala independientes ubicados en hospitales y proveedores de servicios de atención médica, dispositivos médicos en el hogar y unidades de atención en el punto de atención para aplicaciones de atención en el punto de atención remoto, y dispositivos portátiles inteligentes (sensores, actuadores y dispositivos de comunicación) hasta aplicaciones de atención médica móvil e implantes biomédicos.

El IoMT se relaciona estrechamente con eHealth, ya que ambos buscan mejorar la atención médica mediante el uso de tecnología. La eHealth ha florecido en la era de la nube, los dispositivos móviles y el Internet de las cosas (IoT) al proporcionar una amplia variedad de servicios y aplicaciones, incluyendo el mantenimiento de registros de eHealth, medios electrónicos para solicitar pruebas de diagnóstico, prescripción de medicamentos en línea y electrónicamente, sistemas de apoyo a la decisión clínica, telemedicina, gestión del conocimiento en salud, sistemas expertos médicos, procesamiento de imágenes médicas, equipos de atención médica virtual, informática de salud, junto con la investigación orientada a la salud en plataformas de computación en la nube y en la red.

En cuanto al hardware, los dispositivos IoMT incluyen una variedad de equipos médicos, como sensores, dispositivos móviles, bombas de infusión, entre otros, que capturan directamente las indicaciones médicas. Otros dispositivos notables incluyen máquinas de resonancia magnética, bombas de infusión, monitores de pacientes, ventiladores, láser terapéuticos, camas inteligentes y telemetría de la unidad de cuidados intensivos remotos.

Respecto a los protocolos de comunicación, aunque no existen protocolos específicos usados exclusivamente en salud, se sabe que los dispositivos IoMT suelen utilizar una variedad de protocolos de comunicación inalámbrica conocidos para comunicarse. Estos protocolos son Zigbee, Bluetooth, Wi-Fi, WiMAX, LoRA, HART, Sigfox, NB-IoT, entre otros [17].

Finalmente, a pesar de los beneficios significativos que el IoMT puede ofrecer a la atención

médica, también presenta múltiples desafíos. Uno de los más críticos es la privacidad y seguridad de la información que procesan y almacenan estos sistemas. Dado que esta información puede ser altamente sensible (crucial para la vida de una persona o de carácter íntimo), protegerla en dispositivos IoMT, sigue siendo un reto creciente [18]. Además, los recursos limitados de estos dispositivos complican la implementación de algoritmos criptográficos tradicionales, ya que requieren considerable poder de procesamiento y memoria, lo que obliga a utilizar alternativas ligeras que pueden no proporcionar una protección adecuada [19, 20]. La eficiencia energética también es crítica, dado que muchos dispositivos IoMT dependen de baterías, lo que exige protocolos de seguridad energéticamente eficientes, ya que algoritmos que consumen mucha energía pueden reducir la vida útil de los dispositivos [20].

La interoperabilidad entre los diversos dispositivos IoMT y sus protocolos de comunicación es otro desafío importante. La diversidad de plataformas puede generar problemas de compatibilidad, lo que dificulta la implementación de algoritmos de seguridad que funcionen de manera consistente en todos los sistemas, aumentando potencialmente las vulnerabilidades [21]. La proliferación de dispositivos IoMT aumenta las vulnerabilidades y las oportunidades de ataques. Cada dispositivo conectado representa un posible punto de entrada para atacantes, lo que complica la implementación de medidas de seguridad integrales [20]. Si estos dispositivos inteligentes no están debidamente protegidos, pueden comprometer la seguridad de los pacientes y afectar todo el sistema de una organización de atención médica [22].

Otro desafío crucial son los problemas de comunicación. La confiabilidad de los esquemas de transmisión es fundamental, ya que cualquier falla en la transmisión de datos puede tener consecuencias graves para la salud de los pacientes. Las interrupciones en la comunicación pueden resultar en la pérdida de información vital o en la entrega de datos incorrectos, afectando negativamente las decisiones médicas y el tratamiento de los pacientes. Por lo tanto, es esencial que los dispositivos IoMT y los sistemas de comunicación asociados sean altamente confiables y robustos, minimizando las posibilidades de fallos en la transmisión de datos. Además, proteger la integridad de los datos durante su flujo entre múltiples dispositivos es crítico para mantener la privacidad del paciente, aunque resulta difícil garantizarlo [19, 20]. Finalmente, cumplir con regulaciones como HIPAA y GDPR añade una capa adicional de complejidad, ya que los sistemas IoMT deben adaptar continuamente sus medidas de seguridad a medida que evolucionan las normativas [19]. Garantizar la integridad y disponibilidad continua de la información es una prioridad para mantener la eficacia y seguridad de los sistemas de atención médica.

3.1.2. Arquitecturas en eHealth

Las arquitecturas en eHealth buscan organizar la infraestructura (hardware) de manera coherente para facilitar el despliegue y la comprensión de estos sistemas. A lo largo de la literatura relacionada, existen varias arquitecturas propuestas para organizar eHealth. La más común es la arquitectura en tres capas: la Capa de Sensores y Actuadores, la Capa de Borde o "Fog Layer" y la Capa de la Nube. Esta arquitectura busca reducir la latencia y mejorar la calidad de la experiencia (QoE, Quality of Experience) acercando el procesamiento de datos y almacenamiento (dispositivos de borde) a los usuarios finales. Además, facilita aplicaciones de eHealth más personalizadas y eficientes, permitiendo la monitorización remota y en tiempo real de los pacientes. Finalmente, integra tecnologías emergentes como 5G, IoT e IA para

crear una infraestructura robusta y flexible que soporte la creciente demanda de servicios de salud innovadores [23].

Como se explica en [24], los principales beneficios de contar con inteligencia en la capa de borde incluyen:

- *Respuesta en tiempo real*: Las decisiones pueden tomarse de manera más rápida y eficiente al ubicar algoritmos de aprendizaje automático en los dispositivos IoT finales o nodos en el Borde.

- *Reducción del retraso de ida y vuelta (RTT, Round Trip Time)*: Colocar tomadores de decisiones locales en el dispositivo o en el Borde reduce significativamente la frecuencia de contacto con la Nube, lo que resulta en un menor RTT en la toma de decisiones.

- *Reducción del costo de comunicación*: En lugar de enviar datos sin procesar, mediante una fase de preprocesamiento en el Borde, solo se transfieren a los servidores de la Nube retroalimentaciones importantes, alarmas o decisiones. Este enfoque minimiza los costos de comunicación y los gastos generales de mensajes, resultando en costos de comunicación más bajos.

- *Aplicación de políticas locales*: Las regulaciones locales y las políticas de control de acceso pueden aplicarse mejor durante el procesamiento de datos en el Borde, garantizando un cumplimiento más efectivo de los requisitos normativos.

En esta investigación se estudian dos arquitecturas similares. La primera, mostrada en la Figura 3.1, corresponde a una arquitectura de tres capas. Nos referiremos a esta arquitectura como arquitectura de red de área personal por el tipo de comunicación de los dispositivos en el usuario final. En esta arquitectura se consideran los pasos intermedios entre los dispositivos de borde y la nube, incluyendo la estación base y el centro de salud, con una red blockchain en la capa de la nube.

En esta arquitectura, la comunicación entre los dispositivos de recursos limitados (RCD, Resource-Constrained Devices) se realiza directamente con un dispositivo móvil utilizando algún protocolo de comunicación PAN de bajo consumo. Este dispositivo móvil puede ser cualquier computadora con suficientes recursos para procesar la información y enviarla a la estación base. El dispositivo móvil actúa como un concentrador de información y, debido a su proximidad con los dispositivos de recursos limitados, la comunicación tiene un RTT muy bajo. Además, el dispositivo móvil utiliza la infraestructura celular o Wi-Fi, que ofrece una alta velocidad de transmisión y los recursos necesarios para garantizar la fiabilidad. Posteriormente, la información llega a la estación base, donde se deriva a los centros de salud correspondientes. En este punto, la información se procesa a través de la red blockchain y se aplica la inteligencia necesaria en la nube.

La segunda arquitectura abordada en esta investigación, la cual llamaremos arquitectura de LPWAN (Low Power Wide Area Network), se presenta en la Figura 3.2. A diferencia de la arquitectura anterior, los dispositivos sensores se conectan directamente a la estación base mediante un protocolo de bajo consumo y largo alcance. Esta arquitectura, discutida en [8,25], se caracteriza por el uso de tecnologías de comunicación de largo alcance por parte de

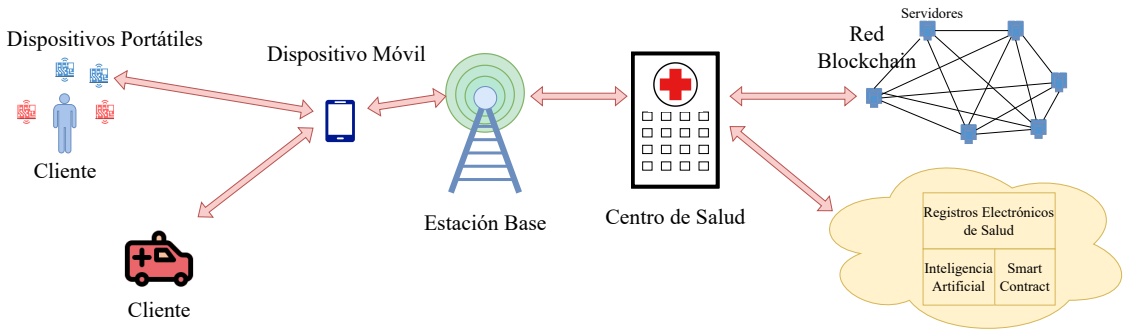


Figura 3.1: Topología simplificada de arquitectura de tres capas.

los dispositivos de recursos limitados. Estas tecnologías, conocidas como LPWAN, presentan numerosos desafíos para lograr una comunicación confiable, los cuales serán revisados más adelante.

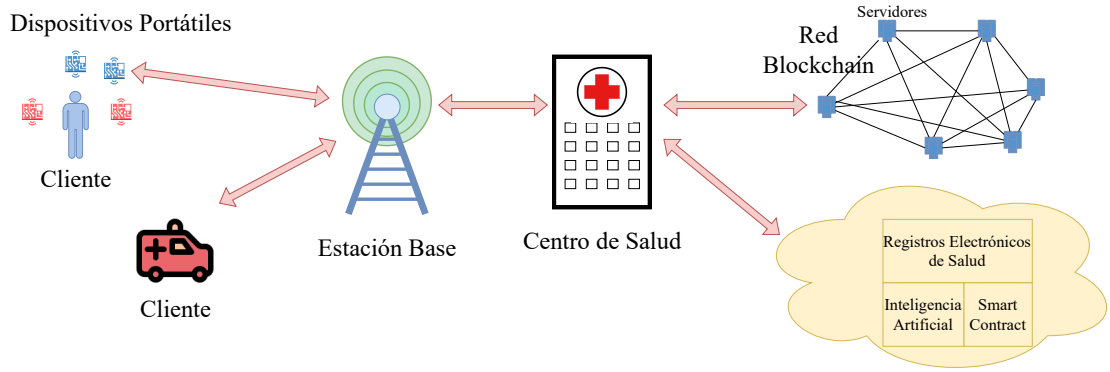


Figura 3.2: Topología simplificada de arquitectura sin dispositivo de borde.

En esta investigación se estudian ambas arquitecturas. De estas, la arquitectura LPWAN será analizada en profundidad por idoneidad en proporcionar fiabilidad en las comunicaciones y proteger la privacidad de la información médica al ser utilizada en los contextos eHealth y ante diferentes escenarios de emergencia

Específicamente, en situaciones de emergencia masiva, los espectros de frecuencia celular suelen fallar, lo que podría resultar en la pérdida de conexión de los dispositivos, un escenario inaceptable para la atención médica remota. Por esta razón, es esencial disponer de una infraestructura dedicada para estos servicios como las tecnologías de comunicación LoRa y Sigfox. Por otro lado, NB-IoT y LTE-M hacen uso de la infraestructura celular pero utilizan diferentes recursos de red, por lo que no deberían verse afectados por emergencias masivas. Todas estas tecnologías ofrecen comunicación de largo alcance y bajo consumo, asegurando que los dispositivos IoMT mantengan una conexión constante y confiable con la estación base, independientemente de las condiciones externas.

3.1.3. Protocolos de Comunicación

En esta subsección se revisarán los principales protocolos de comunicación utilizados en IoMT. Dado que los dispositivos IoMT son un subconjunto del ecosistema IoT, sus comunicaciones confían en protocolos específicos diseñados para este propósito [26]. Los protocolos de comunicación utilizados en IoMT se clasificarán según las dos arquitecturas presentadas en la sección de arquitecturas. Primero, se presentarán los protocolos de área personal más utilizados en la primera arquitectura y, posteriormente, los protocolos de largo alcance y bajo consumo predominantes en la arquitectura LPWAN.

Protocolos PAN (Personal Area Network)

BLE (Bluetooth Low Energy) es ampliamente utilizada para la comunicación en corto alcance en aplicaciones IoMT. BLE es ideal para dispositivos portátiles y sensores que requieren comunicación frecuente pero de bajo consumo de energía. Esta tecnología permite la conexión de dispositivos médicos portátiles, como monitores de ritmo cardíaco y dispositivos de fitness, a teléfonos inteligentes y otros dispositivos de recopilación de datos. BLE proporciona una comunicación eficiente en términos de energía y es compatible con una amplia gama de dispositivos móviles [27].

Wi-Fi es una tecnología de comunicación de rango medio basada en la familia de estándares IEEE 802.11. Es ampliamente utilizada en dispositivos portátiles y para la creación de redes de área local que soportan acceso a Internet para múltiples dispositivos. Aunque WiFi no siempre es adecuado para aplicaciones IoT debido a su relativamente alto consumo de energía, su alta tasa de transferencia de datos lo hace adecuado para aplicaciones IoMT que requieren transmisión de grandes volúmenes de datos, como la telemedicina y la transmisión de video en tiempo real [28].

Zigbee es otra tecnología basada en el estándar IEEE 802.15.4, diseñada para ofrecer comunicación de bajo consumo de energía y baja tasa de datos en redes de área personal. Zigbee es ideal para aplicaciones de monitoreo ambiental y de salud en tiempo real dentro de instalaciones médicas, proporcionando una comunicación fiable y segura en dispositivos IoMT con restricciones de energía [29].

UWB (Ultra-Wideband) es una tecnología de comunicación de corto alcance y alta velocidad, ideal para aplicaciones en entornos hospitalarios donde se requiere una alta precisión y baja interferencia. UWB es adecuada para la transmisión de datos desde sensores implantados a microcontroladores y es utilizada en procedimientos médicos como electrocardiogramas, donde se necesita una comunicación de corto alcance y alta precisión [26].

Protocolos LPWAN (Low Power Wide-Area Network)

Sigfox es una tecnología de red de área amplia de baja potencia (LPWAN) diseñada para comunicaciones de largo alcance y bajo consumo de energía. Ideal para aplicaciones que requieren la transmisión de pequeñas cantidades de datos a intervalos regulares, Sigfox se destaca por su simplicidad, bajo costo y capacidad para operar eficazmente tanto en áreas rurales como urbanas. Esta tecnología es especialmente útil en aplicaciones de seguimiento de ubicación y monitoreo de parámetros básicos de salud, donde la eficiencia energética es

crucial [30]. La capacidad de Sigfox para manejar grandes distancias de comunicación y su eficiencia en términos de consumo de energía lo hacen adecuado para dispositivos IoMT que necesitan transmitir datos con poca frecuencia [31]. Sin embargo, la interoperabilidad de Sigfox es limitada debido a su infraestructura propietaria, lo que significa que solo dispositivos compatibles con Sigfox pueden comunicarse dentro de su red. Además, su latencia es relativamente alta, con tiempos de respuesta que pueden oscilar entre 10 segundos y varios minutos, lo que la hace inadecuada para aplicaciones que requieren transmisión en tiempo real.

LoRa (Long Range) es otra tecnología LPWAN que permite la comunicación inalámbrica a larga distancia con un consumo de energía extremadamente bajo. Utiliza bandas de frecuencia no licenciadas, lo que permite su implementación sin costos adicionales por el uso del espectro. LoRa es conocida por su capacidad de penetrar obstáculos y su robustez en entornos urbanos densos. En el contexto de IoMT, LoRa se emplea para monitorear la salud de pacientes en hogares y hospitales, así como para la gestión de activos médicos. La tecnología proporciona una larga vida útil de la batería, lo que la hace ideal para dispositivos portátiles y sensores remotos. Además, su capacidad de adaptarse dinámicamente a diferentes tasas de datos optimiza su eficiencia en diversas condiciones operativas [30, 32]. LoRaWAN, que es el protocolo de red para LoRa, ofrece un alto grado de interoperabilidad, ya que los dispositivos que cumplen con las especificaciones de LoRaWAN pueden funcionar dentro de cualquier red LoRaWAN. En cuanto a la latencia, LoRaWAN tiene una latencia moderada, que varía entre 1 y 10 segundos, lo que puede ser suficiente para algunas aplicaciones de salud, pero no es adecuada para aquellas que requieren respuestas en tiempo real.

NB-IoT (Narrowband IoT) es un estándar de comunicación LPWAN desarrollado por 3GPP que utiliza bandas de frecuencia licenciadas. Está diseñado para proporcionar una conectividad segura y confiable para dispositivos IoT en entornos urbanos y rurales. NB-IoT es adecuado para aplicaciones de IoMT que requieren la transmisión de grandes volúmenes de datos, como el monitoreo continuo de pacientes crónicos y la gestión de dispositivos médicos en tiempo real. Además, la tecnología es compatible con las redes móviles existentes, lo que facilita su despliegue a gran escala [30]. La robustez y la capacidad de NB-IoT para manejar un gran número de conexiones simultáneas la hacen ideal para infraestructuras de salud inteligentes [32]. En cuanto a interoperabilidad, NB-IoT se integra fácilmente con las redes celulares LTE existentes, permitiendo que dispositivos de diferentes fabricantes interoperables se conecten a una infraestructura común. La latencia en NB-IoT varía entre 1.5 y 10 segundos, lo que lo hace adecuado para aplicaciones que no requieren una respuesta inmediata, pero menos ideal para aquellas que exigen transmisiones en tiempo real.

LTE-M (Long Term Evolution for Machines) es una tecnología LPWAN que ofrece mayores velocidades de datos y una mejor cobertura que NB-IoT, al tiempo que mantiene un bajo consumo de energía. LTE-M es ideal para aplicaciones de IoMT que requieren una alta movilidad y transmisión de datos en tiempo real, como la telemetría de dispositivos médicos móviles y el seguimiento de pacientes en movimiento. Esta tecnología proporciona una mayor capacidad de ancho de banda y menores latencias, lo que la hace adecuada para aplicaciones críticas donde la rapidez en la transmisión de datos es esencial [30]. LTE-M aprovecha la infraestructura de las redes LTE existentes, lo que facilita su implementación y asegura una cobertura global [33]. En términos de interoperabilidad, LTE-M, al igual que NB-IoT, se basa en la infraestructura de redes celulares LTE, lo que permite que dispositivos de múl-

tiples fabricantes operen de manera interoperable a nivel global. Además, LTE-M tiene una latencia baja, entre 50 y 100 milisegundos, lo que lo hace ideal para aplicaciones de salud que requieren respuestas en tiempo real o cercanas al tiempo real.

A continuación se presenta un resumen comparativo de las tecnologías LPWAN en la Tabla 3.1.

3.1.4. Normativas y Regulaciones

IEEE 802.15.6

IEEE 802.15.6 define los requisitos y limitaciones para las redes de área corporal inalámbricas (WBAN), enfocándose en la comunicación de dispositivos cercanos o implantados en el cuerpo humano. El objetivo es establecer un estándar internacional para una comunicación inalámbrica de corto alcance, bajo consumo energético y alta fiabilidad, adecuada para operar en proximidad o dentro del cuerpo humano. Ofrece tasas de datos de hasta 10 Mbps para satisfacer diversas aplicaciones en salud y entretenimiento. Las redes personales actuales no cumplen con las regulaciones médicas ni ofrecen la combinación necesaria de confiabilidad, calidad de servicio (QoS), baja potencia, tasa de datos y no interferencia requeridas para una amplia gama de aplicaciones de WBAN [10]. Si bien la norma IEEE 802.15.6 no está diseñada para dispositivos de largo alcance, sí abarca gran parte los requisitos y limitaciones de los dispositivos IoMT. A continuación, se describen los principales requisitos establecidos por esta norma aplicables a IoMT con comunicación LPWAN:

- *Bajo Consumo de Energía:* IEEE 802.15.6 prioriza el bajo consumo energético como uno de los requisitos esenciales para los dispositivos WBAN, especialmente aquellos diseñados para aplicaciones médicas implantables o vestibles. Aunque la norma no especifica una duración mínima de la batería ni un valor concreto de consumo en potencia, sí establece la necesidad de que los dispositivos operen de manera eficiente para maximizar la vida útil de la batería. Esto se logra mediante la adopción de técnicas como modos de operación de baja energía, protocolos de acceso al medio eficientes, algoritmos de seguridad ligeros y esquemas de modulación adaptativa. Adicionalmente, la norma propone mecanismos de control de potencia para ajustar dinámicamente el nivel de transmisión, minimizando el consumo según la distancia y la calidad del enlace. Estas consideraciones permiten que los dispositivos WBAN cumplan con los requisitos de uso prolongado, reduciendo la necesidad de reemplazo o recarga frecuente de las baterías, un aspecto crítico en el caso de dispositivos implantados.

- *QoS:* IEEE 802.15.6 establece la calidad de servicio (QoS) como un componente esencial para las redes WBAN, especialmente en aplicaciones médicas donde la entrega oportuna y precisa de los datos es crítica. Para ello, define tres niveles de prioridad de tráfico: normal, alta prioridad y emergencia, permitiendo que los datos críticos tengan preferencia en la transmisión. La norma implementa técnicas de asignación dinámica de recursos, como la asignación de ranuras de tiempo y el control de acceso al medio, para minimizar la latencia y las pérdidas de paquetes. Además, especifica el uso de mecanismos de retransmisión y reconocimiento para asegurar la entrega confiable de los datos, y contempla la adaptación dinámica de las tasas de transmisión y modulación según las condiciones del enlace.

Tabla 3.1: Comparación de características de tecnologías LPWAN: NB-IoT , LoRa, SigFox, y LTE-M.

Características	**NB-IoT** [30, 32]	**LoRa** [30–32, 34]	**SigFox** [30–32]	**LTE-M** [30, 33]
Tecnología	Narrow Band LPWA	Semtech-Long range wireless network	Ultra Narrow Band (UNB)	Long Term Evolution for Machines
Modulación	QPSK, OFDM	CSS (Chirp Spread Spectrum)	DBPSK y GFSK	QPSK
Ancho de Banda	200 kHz	125 kHz o más	100 Hz	1.4 MHz
Tasa Máxima de Datos	Hasta 250 Kbps	50 Kbps	100 bps	Hasta 1 Mbps
Bidireccionalidad	Medio Dúplex	Bidireccional, medio y dúplex completo	Limitado/Medio Dúplex	Bidireccional, medio y dúplex completo
Mensajes Máximos (por día)	Ilimitado	Ilimitado	140 (UL), 4 (DL)	Ilimitado
Longitud Máxima de la Carga Útil	1600 bytes	243 bytes	12 bytes (UL), 8 bytes (DL)	1500 bytes
Rango	Hasta 25 km	Más de 10 km en áreas rurales y 5 km en urbanas	30-50 km (Rural), 3-10 km (Urbano)	Hasta 11 km
Inmunidad a Interferencias	Baja	Muy alta	Muy alta	Alta
Autenticación y Cifrado	No Definido	Autenticación mutua (AES1)	HTTPS en interfaces en la nube de Sigfox	Autenticación mutua (AES)
Tasa de Datos Adaptativa	No Definido	Permitido	No permitido	Permitido
Estandarización	3GPP Rel.13	LoRa Alliance	Colaboración con ETSI	3GPP
Protocolo	Basado en LTE	Protocolo MAC (LoRaWAN)	Protocolo ligero para manejar pequeños mensajes	Basado en LTE
Arquitectura	Celular	Topología en estrella de estrellas	Red en estrella	Celular
Handover	No se realiza en modo conectado; reselcción de celda en modo inactivo	Los dispositivos finales no se unen a una única estación base	Los dispositivos finales no se unen a una única estación base	Soportado
Frecuencia	GSM, LTE Bands	868 MHz, 915 MHz, 433 MHz	868 MHz (EU), 915 MHz (NA), 433 MHz (Asia)	LTE Bands

Asimismo, IEEE 802.15.6 utiliza un enfoque de programación de enlaces basado en intervalos de tiempo (slotted), lo que reduce las colisiones y garantiza el acceso al medio para los datos de alta prioridad. Aunque no define valores fijos para retardo o ancho de banda, la norma incorpora estrategias para optimizar el uso del canal y cumplir con los requisitos de QoS en entornos de comunicación cercanos al cuerpo humano.

- *Seguridad y Privacidad:* IEEE 802.15.6 aborda la seguridad y privacidad en redes WBAN mediante la definición de tres niveles de seguridad: sin seguridad (nivel 0), seguridad con autenticación (nivel 1), y seguridad con cifrado y autenticación (nivel 2). Este enfoque permite proteger la confidencialidad, integridad y autenticidad de los datos, adaptándose a las necesidades de la aplicación. La norma incluye un proceso de asociación segura, que implica la autenticación mutua de los dispositivos para prevenir accesos no autorizados y establecer una clave compartida para el cifrado de datos.

  Asimismo, se recomienda el uso de cifrado simétrico, que es eficiente para dispositivos de baja potencia, y se implementan códigos de autenticación de mensajes (MAC) para verificar la integridad de los datos. La protección contra ataques, como la interceptación y la repetición, se realiza utilizando números de secuencia en los mensajes. Estos mecanismos de seguridad se adaptan a las limitaciones energéticas y computacionales propias de los dispositivos en entornos de eHealth.

- *Interoperabilidad:* La norma IEEE 802.15.6 considera la interoperabilidad como un aspecto clave para las redes WBAN, con el objetivo de permitir que múltiples dispositivos de distintos fabricantes operen en conjunto dentro del mismo entorno de salud. Para ello, la norma define un conjunto de procedimientos de control de acceso al medio (MAC) y protocolos de enlace que aseguran la compatibilidad entre dispositivos. Además, especifica esquemas de direccionamiento y formatos de tramas estándar para la transmisión de datos, facilitando la comunicación entre dispositivos WBAN y otros sistemas de comunicación, como redes Wi-Fi o Bluetooth, al emplear bandas de frecuencia comúnmente usadas en aplicaciones médicas, como la banda de 2.4 GHz ISM.

  IEEE 802.15.6 también incorpora mecanismos para la coexistencia con otras tecnologías inalámbricas, mitigando las interferencias y evitando colisiones de señal. Esto se logra mediante el uso de técnicas como la modulación adaptativa y el control de potencia, que ajustan los parámetros de transmisión de los dispositivos WBAN según las condiciones del entorno, permitiendo así una operación armoniosa con otros sistemas de comunicación cercanos. Aunque la norma no dicta una implementación específica para la interoperabilidad, proporciona las bases para que los desarrolladores aseguren la compatibilidad y la integración de los dispositivos WBAN en infraestructuras de eHealth más amplias.

Por otro lado, la norma impone importantes limitaciones tanto para la comunicación como para los dispositivos empleados en el ámbito de la salud. A continuación, se describen las principales limitaciones establecidas por IEEE 802.15.6 aplicables a IoMT con comunicación LPWAN:

- *Niveles de Radiación:* IEEE 802.15.6 aborda el nivel de radiación máxima que los dispositivos WBAN pueden emitir, enfocándose en garantizar la seguridad y minimizar los posibles efectos adversos sobre el cuerpo humano. La norma especifica que los dispositivos WBAN deben cumplir con las regulaciones internacionales de exposición a radiación electromagnética, como las establecidas por la Comisión Internacional de Protección contra la Radiación No Ionizante (ICNIRP) y las directrices de la Comisión Federal de Comunicaciones (FCC) en los Estados Unidos.

Aunque IEEE 802.15.6 no define un valor específico para el nivel máximo de radiación, enfatiza que los dispositivos deben operar dentro de los límites de potencia de transmisión que cumplan con estos estándares de seguridad. Esto se traduce generalmente en una potencia de transmisión muy baja, adecuada para la corta distancia de comunicación característica de las WBAN, lo que minimiza la exposición del cuerpo a radiación electromagnética y reduce el consumo energético.

Regulaciones Internacionales

El Reglamento General de Protección de Datos (GDPR) y la Ley de Portabilidad y Responsabilidad de Seguros de Salud (HIPAA) son regulaciones internacionales fundamentales para la protección de los datos personales, especialmente en el ámbito de la salud. Estas normativas establecen estrictos requisitos para el manejo, procesamiento y almacenamiento de datos médicos, enfocándose en la privacidad y la seguridad de la información.

El GDPR, aplicable en los países de la Unión Europea, clasifica los datos de salud como una categoría especial de datos personales. El reglamento establece que el procesamiento de estos datos solo es legal si se cumplen ciertos requisitos, como el consentimiento explícito del titular o la necesidad de los datos para la prestación de servicios médicos. Además, el GDPR obliga a las organizaciones a implementar medidas de seguridad avanzadas, como el cifrado y la seudonimización, para proteger los datos durante su almacenamiento y transmisión. También concede a los individuos derechos específicos, como el acceso, rectificación, eliminación y portabilidad de sus datos, lo que obliga a los sistemas de salud a contar con mecanismos que respeten y cumplan con estos derechos [12].

La HIPAA es una regulación de los Estados Unidos que establece estándares para la protección de la información de salud protegida (PHI, Protected Health Information). Esta ley incluye dos reglas clave: la Regla de Privacidad y la Regla de Seguridad. La Regla de Privacidad establece los derechos de los pacientes sobre su información médica y establece restricciones sobre el uso y divulgación de la PHI sin el consentimiento del paciente. La Regla de Seguridad, por otro lado, requiere que las organizaciones implementen medidas técnicas, físicas y administrativas para proteger la confidencialidad, integridad y disponibilidad de los datos electrónicos de salud. Estas medidas incluyen la implementación de controles de acceso, auditorías, procedimientos de autenticación y cifrado de datos [11].

Tanto el GDPR como la HIPAA demandan que las organizaciones de salud sean proactivas en la protección de los datos médicos. Mientras que el GDPR se enfoca en la protección de los datos personales en un sentido más amplio, otorgando derechos significativos a los individuos, la HIPAA se centra específicamente en la protección de la información médica en el contexto de la atención sanitaria en Estados Unidos. Ambos marcos normativos influyen en la manera en que se desarrollan y operan los sistemas de salud electrónicos, asegurando que se tomen en cuenta la privacidad y seguridad del paciente como aspectos fundamentales en el manejo de la información.

Ley de Protección de Datos Personales en Chile

La Ley N° 19.628 sobre Protección de la Vida Privada es la regulación chilena que establece las directrices para el tratamiento de datos personales en el país. Define los datos personales

como cualquier información concerniente a personas naturales, identificadas o identificables, y establece que su tratamiento debe realizarse de forma lícita, con el consentimiento expreso del titular. Dentro de esta ley, los datos sensibles se definen como aquellos datos personales que se refieren a las características físicas o morales de las personas, tales como hábitos personales, origen racial, ideologías y opiniones políticas, creencias o convicciones religiosas, estados de salud físicos o psíquicos y la vida sexual [13]. La ley exige que quienes manejen estos datos implementen medidas de seguridad para evitar su pérdida, adulteración o acceso no autorizado, aunque no especifica qué mecanismos o tecnologías se deben emplear. Además, otorga a los titulares derechos específicos, como el acceso, rectificación, cancelación y oposición al tratamiento de sus datos, obligando a las entidades que los manejan a establecer procedimientos claros para responder a estas solicitudes. Actualmente, la ley se encuentra en proceso de actualización para alinearse con estándares internacionales, como el GDPR, y así fortalecer la protección y privacidad de los datos personales en Chile.

3.2. Esquemas de Transmisión

Los esquemas de transmisión varían según las características de la comunicación y dependen de las condiciones del canal y los requisitos específicos, como la velocidad, la fiabilidad, la disponibilidad y la seguridad, entre otros. En esta investigación, se estudian los esquemas de comunicación para dispositivos de recursos limitados en el ámbito de eHealth. Este tipo de comunicación requiere una alta fiabilidad para evitar retransmisiones y niveles de seguridad que garanticen la confidencialidad, integridad, autenticidad, no repudio y privacidad de la información. Para asegurar estas propiedades, es esencial desarrollar un esquema criptográfico robusto, que considere los requerimientos de comunicación intrínsecos del ámbito eHealth.

La evaluación de la confiabilidad de la comunicación se puede comparar de manera efectiva mediante el análisis de la métrica de probabilidad de interrupción [35]. La probabilidad de interrupción se puede definir como el momento en que el nivel de potencia del receptor cae por debajo de un umbral especificado. Este nivel de potencia está asociado con la relación señal-ruido mínima (SNR) dentro de una red inalámbrica. En este contexto, se puede decir que el receptor ya no está dentro del rango de cobertura de la estación base en comunicaciones inalámbricas [36]. En las comunicaciones inalámbricas, existen dos enfoques principales para disminuir la probabilidad de interrupción: reducir la tasa de transmisión o incorporar redundancia en los mensajes.

Abordar el desafío de reducir la tasa de transmisión presenta dificultades, a menudo requiriendo un compromiso, como disminuir la información esencial crucial para el funcionamiento adecuado de los esquemas de transmisión, incluyendo la sobrecarga o el envío de menos información por intervalo de tiempo. Alterar la tasa de transmisión también tendrá un impacto en la antigüedad de la información, como se discute en [37]. Por lo tanto, la relación de frescura de la información (FRoI) [38] necesita ser evaluada según la nueva tasa de transmisión. Modificar la tasa de transmisión puede impactar la seguridad y el rendimiento de los dispositivos de baja potencia. Por el contrario, aumentar la redundancia de la información puede reducir la probabilidad de interrupción con mínimos inconvenientes.

La técnica más sencilla para introducir redundancia implica la repetición de mensajes, mejorando la probabilidad de recepción correcta de la información incluso en presencia de

mensajes perdidos. Dichas estrategias son particularmente favorables en aplicaciones de redes de área amplia de baja potencia (LPWAN), donde asegurar una alta confiabilidad del servicio y acomodar el intercambio de datos tolerante a retrasos son primordiales, como se explica en [39]. Explorando la estrategia de repetición de mensajes, la investigación presentada en [40] establece la existencia de un número óptimo de repeticiones, dependiendo de los recursos de transmisión disponibles. Esto resalta la importancia de adaptar los niveles de redundancia para una mejora eficiente de la comunicación. Además, el documento citado como [41] introduce un innovador esquema de replicación para LPWAN, considerando la capacidad de la pasarela para recuperar señales superpuestas en el dominio de potencia a través de la cancelación sucesiva de interferencias (SIC). Además, el trabajo [25] profundiza en el análisis del rendimiento de los esquemas de transmisión por repetición mejorados con blockchain. Estos esquemas utilizan réplicas exactas de los mensajes para mostrar el equilibrio entre la autenticación oportuna de los bloques y la confiabilidad de la comunicación.

Una estrategia alternativa para introducir redundancia implica la aplicación de la codificación de borrado, con elecciones populares que incluyen los códigos de Reed-Solomon [42], los códigos de baja densidad de paridad (LDPC) [43] y los códigos de fuente [44]. Sin embargo, estas técnicas pueden presentar desafíos debido a su complejidad en el caso de los códigos de Reed-Solomon, limitaciones en la recuperación del mensaje completo para los códigos de paridad, o tasas variables para los códigos de fuente. Abordando la necesidad de simplicidad en la codificación de borrado, se explora una alternativa efectiva en [45], donde dos mensajes pueden generar un mensaje codificado mediante operaciones booleanas. En esta forma de codificación de borrado, incluso si uno de los mensajes no se recibe, aún puede ser recuperado usando el mensaje codificado y el mensaje simple restante. Además, existen enfoques híbridos que combinan tanto la repetición como la codificación, conocidos como replicación codificada híbrida. Estos esquemas seleccionan dinámicamente el método basado en lograr una menor probabilidad de interrupción, demostrando que los esquemas de replicación superan a los otros en canales con alto ruido [46]. Dadas las limitaciones de recursos de los dispositivos en los que se ejecutarán estos esquemas codificados, la simplicidad es crucial. En consecuencia, la generación de mensajes codificados a partir de más de dos mensajes no es recomendable, debido a recursos limitados como la memoria y el tiempo de ejecución.

3.3. Confiabilidad de Canal

La confiabilidad de un canal de comunicación se analiza a través de la relación señal-ruido (SNR), que mide la proporción entre la potencia de la señal recibida $r(t)$ y la potencia del ruido $n(t)$, dentro de un ancho de banda W. En un canal inalámbrico, la SNR instantánea se puede expresar como:

$$\gamma = \frac{P_{\mathrm{t}} g h^2}{N_0 W}, \tag{3.1}$$

donde P_{t} es la potencia de transmisión, g es la ganancia de potencia del canal, h es la magnitud del desvanecimiento, y N_0 es la densidad espectral de potencia del ruido térmico.

La capacidad de canal de Shannon establece el límite máximo de la tasa de transmisión de información libre de errores en un canal ruidoso y está dada por:

$$C = W \log_2 (1 + \gamma), \tag{3.2}$$

donde C es la capacidad del canal en bits por segundo (bps), W es el ancho de banda en Hz y γ es la SNR del canal. Este límite representa la tasa máxima teórica que un canal puede soportar sin errores, bajo condiciones ideales.

En sistemas prácticos, la tasa de transmisión efectiva R_s puede no coincidir con la capacidad teórica de Shannon debido a las limitaciones impuestas por la implementación, como la modulación, codificación y condiciones del canal. Por esta razón, en lugar de utilizar C, se considera la tasa de transmisión efectiva de un sistema particular R_s. A partir de la expresión de Shannon para la capacidad de canal, es posible despejar la relación señal-ruido mínima requerida para soportar una tasa de transmisión R_s:

$$\gamma_s = 2^{\frac{R_s}{W}} - 1, \tag{3.3}$$

donde R_s es la tasa de transmisión en bps y W es el ancho de banda del canal en Hz. Esta ecuación proporciona la SNR mínima necesaria para que el canal soporte la tasa de transmisión R_s.

La probabilidad de interrupción del enlace, conocida como *outage probability*, se refiere a la posibilidad de que la SNR instantánea γ del canal caiga por debajo de un umbral mínimo γ_s, impidiendo una transmisión confiable. Esta probabilidad, que puede expresarse mediante la función de distribución acumulativa, se define como:

$$\mathcal{O}_{link} = P(\gamma < \gamma_s) = \int_0^{\gamma_s} p(\gamma)\,\mathrm{d}\gamma, \tag{3.4}$$

donde $p(\gamma)$ denota la función de densidad de probabilidad de la variable continua γ.

Considerando el desvanecimiento de Rayleigh, la probabilidad de interrupción del enlace se convierte en

$$\mathcal{O}_{link} = 1 - \exp\left(-\left(2^{\frac{R_s}{W}} - 1\right)\frac{N_0 W}{g P_\mathrm{t}}\right), \tag{3.5}$$

donde R_s es la tasa de transmisión, en este caso, equivalente a la capacidad del canal de Shannon para γ_0 [47]. Sin embargo, al considerar transmisiones sobre un canal Nakagami-m, la probabilidad de interrupción del enlace se convierte en

$$\mathcal{O}_{link} = \frac{\Gamma\left(m, m\left(2^{\frac{R_s}{W}} - 1\right)\frac{N_0 W}{g P_\mathrm{t}}\right)}{\Gamma(m)}, \tag{3.6}$$

donde $\Gamma(m, x) = \int_0^x y^{m-1}\exp(-y)\mathrm{d}y$ es la función gamma incompleta mientras que $\Gamma(m) = \int_0^\infty y^{m-1}\exp(-y)\mathrm{d}y$ es la función gamma completa, respectivamente [48]. Dado que el modelo de desvanecimiento Nakagami-m incluye a Rayleigh como un caso especial, con $m = 1$, que constituye el peor caso en la probabilidad de interrupción del enlace, los resultados se referirán al canal de Rayleigh a menos que se indique lo contrario [47].

3.4. Criptografía

Hoy en día, la criptografía está compuesta por una gran variedad de algoritmos que buscan dotar de confidencialidad, integridad y autenticidad a la información. La confidencialidad es

la propiedad de la información de ser entendida solo por aquellos a quienes les corresponde. Por otro lado, la integridad de la información busca garantizar que la información se encuentre completa e idéntica a como fue enviada. Finalmente, la autenticidad es la propiedad de la información que la asocia a un emisor de forma inequívoca, de esta forma tener garantía de que el mensaje fue generado por el emisor correspondiente. Antes de profundizar en los diferentes tipos de algoritmos criptográficos, es importante entender cómo se mide la seguridad de los cifrados. La seguridad de un cifrado se evalúa en función de la resistencia a los ataques criptoanalíticos, es decir, la dificultad que tendría un atacante para romper el cifrado y acceder a la información protegida. En un buen algoritmo criptográfico el mejor ataque no debe ser mejor que un ataque de fuerza bruta a la clave. Debido a esto es que la dificultad se mide en términos de la cantidad de combinaciones que debe probar el atacante para encontrar la clave secreta con un 100 % de probabilidad, y se expresa en bits. Por ejemplo, una seguridad de 128 bits significa que el atacante tendría que probar 2^{128} combinaciones (aproximadamente $3{,}4 \times 10^{38}$ combinaciones) para romper el cifrado. Dentro de lo que se conoce como criptografía moderna, podemos encontrar algoritmos de cifrado simétrico y asimétrico, así como algoritmos de hash. Con estos cifrados se construyen muchos servicios de seguridad e implementaciones criptográficas. En las siguientes subsecciones se abordarán los distintos algoritmos criptográficos y una de sus implementaciones más conocidas, el blockchain.

3.4.1. Criptografía Simétrica

La criptografía simétrica tiene como objetivo proporcionar confidencialidad a la información. Se denomina simétrica porque tanto el emisor como el receptor comparten una clave secreta que se utiliza para cifrar y descifrar, como se muestra en la Figura 3.3.

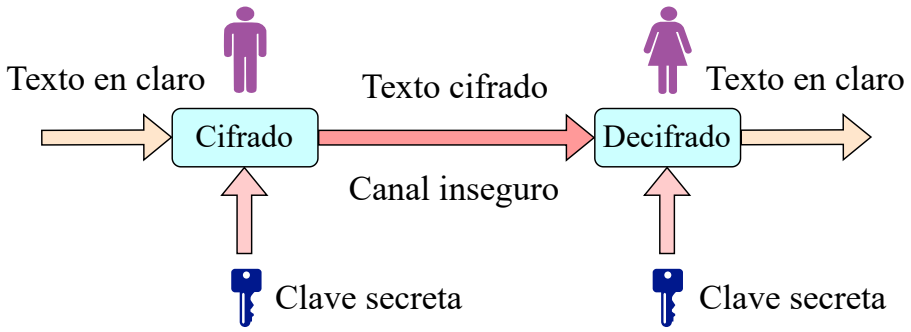


Figura 3.3: Comunicación con un cifrado simétrico por un canal inseguro.

La principal ventaja de la criptografía simétrica radica en la velocidad y eficiencia del procesamiento de datos, lo que permite realizar operaciones de cifrado y descifrado de manera rápida. Varios estudios se han centrado en el rendimiento de los cifrados simétricos [6, 7, 49–57]. Sin embargo, realizar una comparación justa entre ellos es un desafío debido a que, al utilizar diferentes plataformas de prueba, los resultados varían considerablemente entre investigaciones. Las métricas de comparación más comunes incluyen el uso de RAM, el uso de memoria flash, el rendimiento, el tiempo, el consumo de energía, la cantidad de tablas de búsqueda necesarias y los diferentes niveles de optimización para cada cifrado. Como se explica en [8], es evidente que AES [58] es la opción más frecuentemente elegida.

Al comparar AES con varios algoritmos de criptografía ligera (LWC, Lightweight Cryptography), estos últimos son más rápidos, requieren menos cantidad de memoria y consumen menos energía. Sin embargo, como se concluye en [6,7], estos algoritmos aún no cumplen con los requisitos de seguridad necesarios, siendo actualmente vulnerables a varios ataques.

Sin embargo, en el año 2019 se finalizó la competencia CAESAR para criptografía autenticada, donde Ascon fue uno de los ganadores en la categoría de cifrados autenticados para hardware restringido [59]. Aunque Ascon parece ser un sucesor prometedor de AES en dispositivos de baja potencia, en [57] se concluyó que ACORN es superior a Ascon v1 al usar AES-GCM como punto de referencia, lo que plantea dudas sobre si Ascon es realmente el reemplazo indicado. Hasta este punto, consideramos que estos cifrados ligeros deben someterse a pruebas de seguridad más exhaustivas antes de ser considerados un reemplazo seguro de AES en sistemas embebidos.

En abril de 2022, el NIST concluyó su competencia para identificar un cifrado adecuado para la categoría de Criptografía Ligera [60]. El objetivo era encontrar un cifrado que mantuviera altos estándares de seguridad y fuera altamente eficiente en dispositivos con recursos limitados. El ganador de esta competencia fue la suite de algoritmos criptográficos conocida como Ascon. Debido al extenso prontuario de validaciones en competencias y pruebas realizadas durante y después de la competencia de Criptografía Ligera, consideramos que Ascon es un reemplazo suficientemente validado para emplearse en dispositivos de bajo consumo.

A continuación, se revisará Ascon en detalle, ya que será el algoritmo criptográfico implementado en nuestra propuesta. Ascon incluye cinco variantes: Ascon-128, Ascon-128a, Ascon-HASH, Ascon-XOF y Ascon-80pq. En esta sección, nos centraremos principalmente en Ascon-128 y Ascon-128a, que son cifrados simétricos autenticados. Ambos utilizan claves de 128 bits y producen un texto cifrado del mismo largo que el texto en claro más un tag. Ascon-128 procesa textos en claro de 64 bits, mientras que Ascon-128a procesa textos en claro de 128 bits [61]. La representación del cifrado con Ascon se muestra en la siguiente fórmula:

$$E_{k,r,a,b}(K, N, A, P) = (C, T), \tag{3.7}$$

donde k, r, a y b son parámetros que definen el funcionamiento del cifrado. k representa la longitud de la clave secreta utilizada en los procesos de cifrado y descifrado, r indica el tamaño del bloque de datos procesado en cada ronda del algoritmo, a indica el número de rondas utilizadas en la fase de inicialización de la permutación y b se refiere al número de rondas empleadas en el procesamiento intermedio de datos asociados y texto sin formato. Por otro lado, K, N, A y P son las entradas de la función. La clave K tiene un tamaño máximo de 160 bits y se utiliza para operaciones de cifrado y descifrado en Ascon. El valor N es de 128 bits y se emplea junto con la clave para inicializar el estado de Ascon. A son datos adicionales que pueden autenticarse junto con el mensaje de texto sin formato durante el proceso de cifrado de Ascon, mientras que P es el mensaje original que debe cifrarse. Finalmente, C representa el mensaje cifrado obtenido tras aplicar el algoritmo de cifrado al texto sin formato mediante una clave secreta, y T es una información generada durante el proceso de cifrado que sirve como identificador único del texto cifrado (tag). Ayuda a verificar la autenticidad e integridad del mensaje cifrado y de los datos asociados, asegurando que no

haya sido manipulado durante la transmisión o el almacenamiento.

El proceso de descifrado se representa con la siguiente fórmula:

$$D_{k,r,a,b}(K, N, A, C, T) \in \{P, \perp\}, \tag{3.8}$$

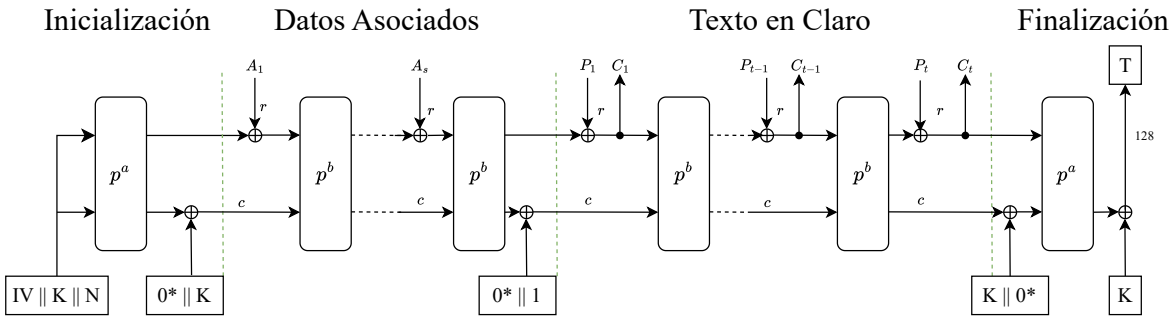
donde la fórmula genera el texto plano P si la verificación de la etiqueta es correcta o un error $\perp$ si la verificación de la etiqueta falla.

En el capítulo 5 se presentan los resultados de la comparación realizada entre cifrados, donde los cifrados simétricos comparados son aquellos que procesan bloques de texto en claro de 128 bits, específicamente AES-128 y Ascon-128a. Por esta razón, profundizaremos en Ascon-128a, para el cual los parámetros recomendados se muestran en la Tabla 3.2.

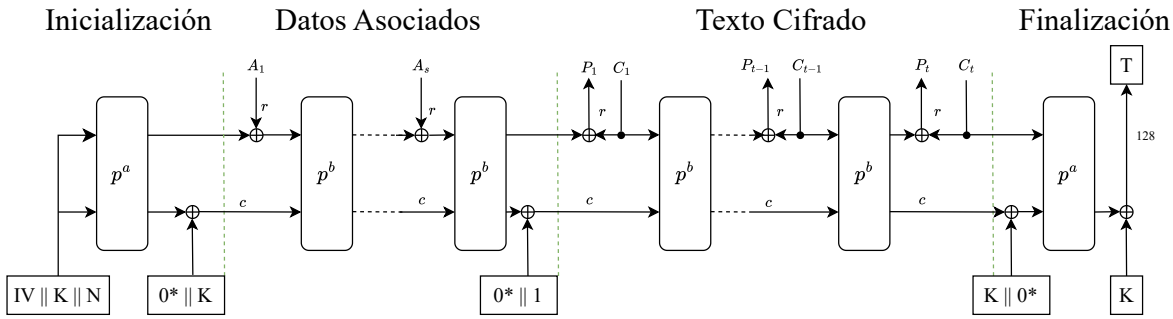
Tabla 3.2: Parámetros recomendados para Ascon-128a.

Nombre	**Algoritmos**	**Tamaño en bits de**				**Rondas**	
		Clave	**Nonce**	**Etiqueta**	**Datos**	p^a	p^b
Ascon-128a	$E, D_{128,128,12,8}$	128	128	128	128	12	8

Ascon se caracteriza por ser un cifrado tipo esponja muy rápido, que utiliza pocos recursos y es fuerte contra ataques de canal lateral. Para entender esto, revisaremos en detalle su estructura y cómo logra su cometido. La estructura se muestra en la siguiente Figura:



a.) Cifrado $\xi_{k,r,a,b}$



b.) Descifrado $D_{k,r,a,b}$

Figura 3.4: Estructura del cifrado Ascon. a.) Proceso de cifrado. b.) Proceso de descifrado.

Se observa que en todas las secciones del algoritmo se trabaja con un bloque p y este se repite a o b veces dependiendo del momento del cifrado en el que nos encontramos. Este bloque p consta de tres funciones principales: la capa de adición de constantes (*Addition of Constants*), la capa de sustitución no lineal (*Substitution Layer*) y la capa de difusión lineal (*Linear Diffusion Layer*). La capa de adición de constantes se encarga de añadir constantes de ronda al estado, la capa de sustitución aplica una caja S para proporcionar no linealidad y la capa de difusión lineal asegura una mezcla adecuada de los bits dentro de cada palabra de 64 bits del estado. Estas capas trabajan conjuntamente para asegurar que cada bit del estado final esté influenciado por cada bit del estado inicial, proporcionando así una alta seguridad contra ataques criptográficos.

Los componentes principales de los esquemas Ascon, Ascon-Xof y Ascon-Hash son las dos permutaciones de 320 bits p^a y p^b. Las permutaciones aplican iterativamente una transformación de ronda basada en SPN (Substitution-Permutation Network) p que a su vez consta de tres pasos: p_C, p_S, y p_L:

$$p = p_L \circ p_S \circ p_C, \tag{3.9}$$

p^a y p^b se diferencian únicamente en el número de rondas. El número de rondas a y el número de rondas b son parámetros de seguridad ajustables.

- **Capa de Adición de Constantes (p_C)**: Esta capa se encarga de añadir constantes de ronda al estado interno del cifrado. La adición de constantes asegura que cada ronda del cifrado sea distinta, lo que incrementa la resistencia contra ataques que intenten explotar patrones repetitivos en las rondas.

- **Capa de Sustitución No Lineal (p_S)**: Esta capa aplica una caja S (S-box) al estado interno del cifrado para proporcionar no linealidad. La sustitución no lineal es crucial para la seguridad del cifrado, ya que introduce complejidad y confusión, dificultando que un atacante pueda predecir o revertir el estado del cifrado. Una contramedida efectiva contra ataques de canal lateral es evitar el uso de tablas de búsqueda (lookup tables) y en su lugar utilizar un equivalente matemático que permite trabajar bit a bit, esta contramedida viene bien definida en el documento oficial de Ascon [61].

- **Capa de Difusión Lineal (p_L)**: Esta capa asegura una mezcla adecuada de los bits dentro de cada palabra de 64 bits del estado. La difusión lineal distribuye la influencia de cada bit del estado inicial a lo largo de todo el estado final, incrementando la seguridad contra ataques diferenciales y lineales.

Ahora que tenemos los ingredientes principales de Ascon definiremos cada una de las secciones:

- **Inicialización**: La inicialización es la fase inicial en el proceso de cifrado de Ascon, donde se prepara el estado interno del cifrado para procesar los datos asociados y el texto plano. Durante esta fase, el estado interno de 320 bits se configura utilizando el vector de inicialización (IV), la clave secreta K y el nonce N. El vector de inicialización (IV) es un valor predeterminado que asegura que cada instancia del cifrado Ascon comienza con un estado interno bien definido. La clave K es un valor secreto de 128 bits utilizado para cifrar y descifrar los datos, mientras que el nonce es un valor único de 128 bits utilizado en cada operación de cifrado para asegurar que, incluso si se cifra el mismo texto plano varias veces con la misma clave, los textos cifrados resultantes serán diferentes. El proceso de inicialización comienza concatenando el IV, la clave K y el nonce N, llenando así el estado interno de 320 bits. Posteriormente, se aplican las permutaciones p^a para mezclar completamente estos valores dentro del estado interno, asegurando que cualquier bit del estado final dependa de cada bit de la clave y el nonce. Finalmente, una operación XOR se realiza entre la clave K y el estado interno, completando el proceso de inicialización y proporcionando una base sólida para la seguridad del cifrado.

- **Datos Asociados (Associated Data)**: En el cifrado autenticado, los datos asociados (AD) son una parte esencial del proceso de autenticación, aunque no se cifran. Estos datos pueden incluir encabezados de paquetes, direcciones de red, o cualquier otro tipo de información que deba ser autenticada pero no protegida contra la divulgación. En Ascon, los datos asociados se procesan junto con el texto plano para generar una

etiqueta de autenticación que garantiza la integridad y autenticidad de los datos. Este enfoque asegura que cualquier modificación en los datos será detectada durante el proceso de verificación, proporcionando una capa adicional de seguridad.

- **Texto Cifrado (Ciphertext)**: El texto cifrado C es el resultado de aplicar el algoritmo de cifrado Ascon al texto plano P. El texto cifrado se genera combinando el estado interno del cifrado con el texto plano utilizando operaciones de XOR en cada iteración de la permutación p en esta sección. Este texto cifrado se transmite junto con el tag de autenticación para asegurar tanto la confidencialidad como la integridad de los datos.

- **Finalización**: La finalización es la fase en la que se genera el tag de autenticación T. Durante esta fase, el estado interno del cifrado, que ya ha procesado los datos asociados y el texto plano, se somete a una serie de permutaciones p^a adicionales. El resultado final es una etiqueta de autenticación que garantiza la integridad y autenticidad de todo el mensaje. Este tag se envía junto con el texto cifrado para permitir la verificación por parte del receptor.

Por todo lo anteriormente mencionado, se puede inferir que Ascon es una alternativa segura y eficiente para dispositivos de recursos limitados. Sin embargo, para validar su eficiencia, Ascon es sometido a rigurosas pruebas, cuyos resultados se presentan en el capítulo 5. Es importante destacar que Ascon no está exento del mayor desafío que enfrentan los cifrados simétricos: compartir de manera segura la clave secreta entre el emisor y el receptor. Este proceso plantea un riesgo significativo de seguridad [62]. Cualquier compromiso de la clave compartida puede llevar a un acceso no autorizado a información sensible, lo que hace que la gestión de claves sea un aspecto crítico y delicado en la criptografía simétrica.

3.4.2. Criptografía Asimétrica

La criptografía asimétrica, también conocida como criptografía de clave pública, ofrece un enfoque seguro para el cifrado y descifrado de datos, aunque suele tener un rendimiento más lento en comparación con la criptografía simétrica debido a sus operaciones matemáticas intrincadas. El cifrado asimétrico se basa en pares de claves, una clave pública para el cifrado y una clave privada para el descifrado. Sin embargo, estos algoritmos son frecuentemente empleados como mecanismos de intercambio de claves. Por ejemplo, los algoritmos Diffie-Hellman (DH) permiten la comunicación segura sin necesidad de secretos precompartidos. En la Figura 3.5 se muestra el protocolo de Diffie-Hellman de curva elíptica (ECDH, Elliptic-curve Diffie–Hellman), donde E es la curva elíptica, $\#E$ es el número de puntos (cardinalidad) en la curva elíptica sobre un campo finito, P es un elemento primitivo, y T_{AB} es el secreto compartido entre Alice y Bob.

Dos de los algoritmos de cifrado asimétrico más populares, Rivest-Shamir-Adleman (RSA) y la criptografía de curva elíptica (ECC), pueden utilizarse para el intercambio de claves y ofrecen distintos niveles de seguridad para la transmisión de datos [63]. Numerosos estudios han demostrado que ECC supera a RSA manteniendo el mismo nivel de seguridad. La equivalencia de seguridad establecida indica que cuando ECC genera claves de 256 bits, esto equivale a claves de 3072 bits en RSA y proporciona una seguridad de 128 bits en comparación con AES. En consecuencia, ECC resulta ser mucho más práctica para dispositivos de recursos limitados [64–67].

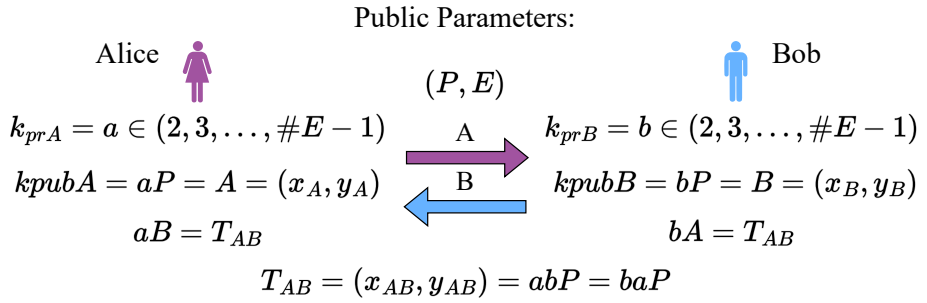


Figura 3.5: Ejemplo de intercambio de claves Diffie-Hellman con curvas elípticas.

Dentro de ECC, existe una variedad de curvas adecuadas para dispositivos IoT. Una curva popular es la secp256r1, debido a su superior eficiencia energética en dispositivos de baja potencia [68]. Esto se debe a las optimizaciones del módulo p para ECC presentadas por NIST [69]. Además, como se muestra en [70], esta curva se implementa en varias bibliotecas para RCD, destacando la biblioteca Micro-ECC como la más rápida y una de las más seguras contra ataques de hardware. Otra curva altamente recomendada por su eficiencia es Curve25519 [71–73]. El estudio en [74] compara Curve25519 y secp256r1, mostrando que Curve25519 puede ser más ventajosa en varios escenarios. Sin embargo, Curve25519 no ha sido tan ampliamente implementada en dispositivos de baja potencia, y hay menos bibliotecas disponibles para su implementación. Además, secp256r1 es la curva recomendada por NIST. Sin embargo, basado en la bibliografía encontrada determinamos que no es trivial la elección entre ambas curvas. Es por esto que en el capítulo 5 se presentan los resultados de pruebas de desempeño realizadas con ambas curvas.

3.4.3. Algoritmos de Hash

Los algoritmos hash, o funciones hash, sirven como herramientas criptográficas para tomar una entrada de longitud variable y transformarla en una cadena de caracteres de longitud fija, típicamente representada en forma hexadecimal o binaria como se muestra en la Figura 3.6. Estos algoritmos se utilizan principalmente para asegurar la integridad de los datos y confirmar la autenticidad de la información a través de la generación de un "digest.º "valor hash"único para una entrada determinada. Una característica crítica de las funciones hash es su capacidad para producir un valor hash significativamente distinto incluso ante pequeñas alteraciones en los datos de entrada [75, 76]. Una colisión es la ocurrencia de dos entradas distintas que producen la misma salida en una función de hash, lo que provoca una brecha en la seguridad. Las funciones de hash de alta calidad están diseñadas para minimizar la probabilidad de colisión, acercándose a cero.

Los algoritmos hash se han utilizado durante muchos años y, con el paso del tiempo, algunos se han vuelto obsoletos. En respuesta a esta preocupación, el NIST inició una competencia abierta para el desarrollo del Algoritmo de Hash Seguro 3 (SHA-3). Para diciembre de 2010, la competencia se había reducido a cinco finalistas: Blake, Grøstl, JH, Keccak y Skein. Finalmente, en octubre de 2012, el algoritmo Keccak fue elegido como el ganador de SHA-3, mientras que los cinco finalistas continuaron encontrando aplicaciones basadas en sus fortalezas distintivas [77].

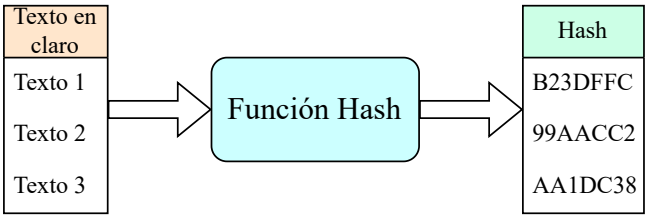


Figura 3.6: Ejemplo genérico de Hashing.

Entre estos finalistas, Blake ha demostrado un rendimiento encomiable en dispositivos de recursos limitados. Dos versiones más recientes de Blake, Blake2s y Blake3, han mostrado un rendimiento superior en términos de ciclos por byte, independientemente del tamaño de la entrada o del hash [78]. Blake3 ha mostrado un rendimiento ligeramente mejor en ciclos por byte, mientras que Blake2s tiene un tamaño de código más pequeño. En la investigación [79], se realiza un estudio de varios hashes ligeros, destacando a PHOTON como el más equilibrado. Sin embargo, la comparación utilizó paralelismo en todos los algoritmos, lo cual no es factible para todos los RCD. Además, a pesar de mencionar el algoritmo Blake, no se incluyó entre los algoritmos comparados. En el estudio [8], Blake2s fue seleccionado como el algoritmo de hash más indicado para dispositivos de recursos limitados.

En la competencia concluida en 2022, enfocada en Criptografía Ligera, se presentó la suite del algoritmo Ascon, que incluye dos algoritmos hash: Ascon-Hash y Ascon-XOF. Ascon-Hash y Ascon-XOF son variantes del algoritmo Ascon, diseñadas para satisfacer diferentes necesidades criptográficas. Ascon-Hash es una función de hash estándar que toma una entrada de longitud arbitraria y produce una salida de longitud fija, generalmente de 256 bits. Esta característica lo hace ideal para aplicaciones donde se necesita un valor hash consistente, como la verificación de integridad de datos, firmas digitales y otras aplicaciones donde un valor de hash fijo es suficiente y necesario. Por otro lado, Ascon-XOF (eXtendable Output Function) ofrece una salida de longitud variable, lo que proporciona mayor flexibilidad para generar la cantidad exacta de datos requerida. Esto es particularmente útil en escenarios criptográficos avanzados, como la generación de números pseudoaleatorios, la expansión de claves criptográficas y cualquier aplicación que requiera una salida que no esté predefinida en longitud.

Mientras que Ascon-Hash se centra en la producción de un valor hash fijo y consistente para aplicaciones tradicionales de hash, Ascon-XOF expande su utilidad al permitir que los usuarios especifiquen la longitud de la salida según las necesidades del contexto. Esta diferencia fundamental en el manejo de la salida convierte a Ascon-Hash en una opción robusta para tareas estándar de hashing, mientras que Ascon-XOF se posiciona como una herramienta versátil y adaptable para aplicaciones criptográficas que demandan flexibilidad en la longitud de los datos generados. En conjunto, ambos esquemas ofrecen soluciones complementarias dentro del ecosistema Ascon, asegurando tanto la seguridad como la eficiencia en una amplia gama de aplicaciones criptográficas. Estos algoritmos cumplen con los estándares de seguridad suficientes y son implementables en todo tipo de dispositivos [61].

Consideramos necesario realizar una comparación en profundidad del desempeño de Ascon-Hash y Blake2s en dispositivos de recursos limitados antes de determinar cuál es el hash más

adecuado. Es por esto, que en el capítulo 5 se entregan resultados de una comparación de desempeño llevada a cabo.

3.4.4. Firmas Digitales y Código de Autenticación de Mensajes

Una firma digital es una técnica criptográfica utilizada para lograr la autenticidad, no repudio e integridad de la información. Implica el uso de una clave privada para crear una huella digital o firma única para el contenido, que luego puede ser verificada por cualquier persona con acceso a la clave pública correspondiente. Las firmas digitales proporcionan una forma segura de asegurar que el remitente de la información es legítimo y que los datos no han sido alterados durante la transmisión [75, 76]. El proceso dde firma digital se muestra en la Figura 3.7.

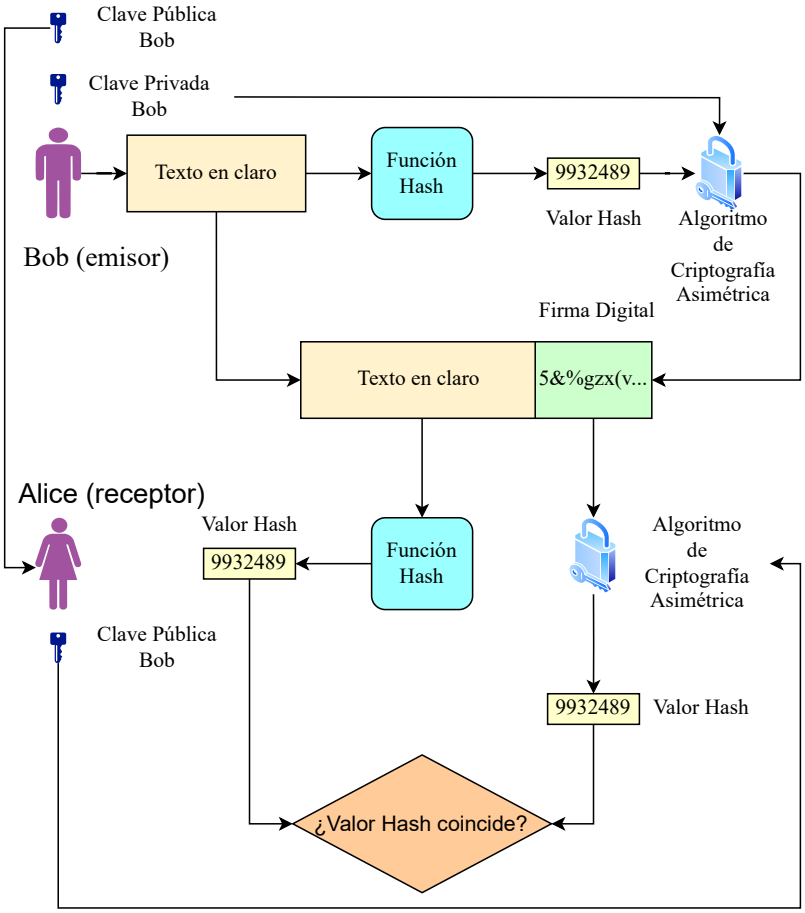


Figura 3.7: Ejemplo genérico de firma digital.

Existe una herramienta criptográfica similar a las firmas digitales conocida como código de autenticación de mensaje (MAC, Message Authentication Code). Un MAC es un pequeño bloque de datos generado a partir de un mensaje utilizando una clave secreta, que se añade al mensaje para garantizar tanto su integridad como su autenticidad. Al igual que una firma digital, un MAC asegura la integridad y la autenticidad del mensaje. Sin embargo, a diferencia

de las firmas digitales, los MAC no proporcionan no repudio y utilizan criptografía simétrica. Utilizar MAC es más eficiente computacionalmente hablando, ya que se evita en gran medida el uso de criptografía asimétrica, que es más costosa en términos computacionales.

Además, los MAC no otorgan no repudio debido a que tanto el emisor como el receptor usan la misma clave para firmar, lo que significa que no se puede determinar quién envió el mensaje y uno podría hacerse pasar por el otro. En caso de que uno de los involucrados en la comunicación sea completamente confiable, y la clave secreta solo sea compartida entre dos partes, se puede conseguir algo conceptualmente distinto al no repudio pero muy parecido en la práctica. En la Tabla 3.3 se resumen las diferencias entre firmas digitales y MAC.

Existen tres enfoques principales para utilizar MACs: MAC-luego-cifrado, Cifrado-y-MAC, y Cifrado-luego-MAC. El enfoque de Cifrado-luego-MAC es el más ampliamente aceptado, ya que generalmente ofrece mejor eficiencia. Esto se debe a que al verificar los mensajes no es necesario descifrar el mensaje, ya que el MAC se realiza sobre el mensaje cifrado. Si el MAC no coincide, el mensaje puede ser descartado sin necesidad de descifrarlo, lo que ahorra recursos computacionales. Además, este enfoque ha demostrado ser más robusto ante algunos tipos de ataques criptográficos.

Tabla 3.3: Comparación entre Firma Digital y MAC.

Característica	**Firma Digital**	**MAC**
Criptografía	Asimétrica	Simétrica
Propósito	Integridad, autenticidad, no repudio	Integridad, autenticidad
Generación	Cifrado del hash con clave privada	Uso de una clave secreta y un algoritmo MAC
Verificación	Descifrado con clave pública	Uso de la misma clave secreta
Aplicaciones	Firmas electrónicas, certificados digitales	Autenticación de mensajes, protección de datos

Existen otras variantes de firmas digitales muy atractivas como el concepto de firmas agregadas presentado en [80]. Una firma agregada permite que más de una identidad sea validada dentro de una sola firma, es decir, varios firmantes o varios bloques de información podrían ser validados con una única firma. En [81], se sugiere la utilización de firmas agregadas para dispositivos con recursos limitados basadas en ECC. No obstante, los experimentos se realizaron en una computadora de alto rendimiento. De manera similar, en [82], se introducen esquemas de firmas agregadas que emplean mapas bilineales para dispositivos con recursos limitados. Sin embargo, en este estudio, los resultados también se obtuvieron utilizando dispositivos de alto rendimiento, y es ampliamente reconocido que los mapas bilineales son excesivamente demandantes computacionalmente para dichos dispositivos con recursos limitados. Es por estas razones que consideramos que las firmas agregadas no son adecuadas para dispositivos de recursos limitados pero si para dispositivos de la capa de borde en adelante. Un tipo de firma agregada muy atractiva para dispositivos con altas prestaciones son las firmas BLS (Boneh-Lynn-Shacham) que permiten saber si un firmante pertenece a la firma sin conocer las firmas de los demás involucrados [83, 84].

3.4.5. Blockchain

La tecnología blockchain funciona como un sistema de transacciones que mantiene un registro de todas las transacciones. Periódicamente, estas transacciones generan bloques, cada uno de los cuales pasa por un proceso de validación. Si un bloque pasa con éxito esta validación, establece una conexión con el bloque anterior, convirtiéndose en parte del registro. Esta conexión puede ser el valor hash del bloque anterior, creando una cadena de bloques ininterrumpida. La Figura 3.8 proporciona una representación visual del encadenamiento de bloques. Si un bloque no supera la validación, se descarta. El proceso de validación de nuevos bloques se logra a través de un método de consenso como la prueba de trabajo (PoW) utilizada en Bitcoin [85], que implica resolver un rompecabezas computacionalmente intensivo. Resolver estos rompecabezas es altamente complejo y demandante computacionalmente, lo que resulta en un consumo significativo de energía [86, 87]. Se han explorado diversos métodos, como la prueba de participación o mecanismos de consenso mixtos para mejorar la eficiencia energética en la validación de bloques.

Blockchain tiene variadas aplicaciones en la seguridad médica, principalmente en la gestión y protección de datos de salud. Permite crear registros inmutables y descentralizados para las historias clínicas electrónicas (EHR), asegurando la integridad y autenticidad de la información, además de ofrecer a los pacientes control sobre quién puede acceder a sus datos. También facilita el intercambio seguro de información médica entre diferentes proveedores de salud, garantizando la privacidad mediante contratos inteligentes. En la cadena de suministro de medicamentos, blockchain rastrea cada etapa para prevenir la introducción de medicamentos falsificados. Asimismo, se utiliza en ensayos clínicos para registrar datos de manera segura y en la gestión de consentimientos médicos, creando un historial auditable y transparente.

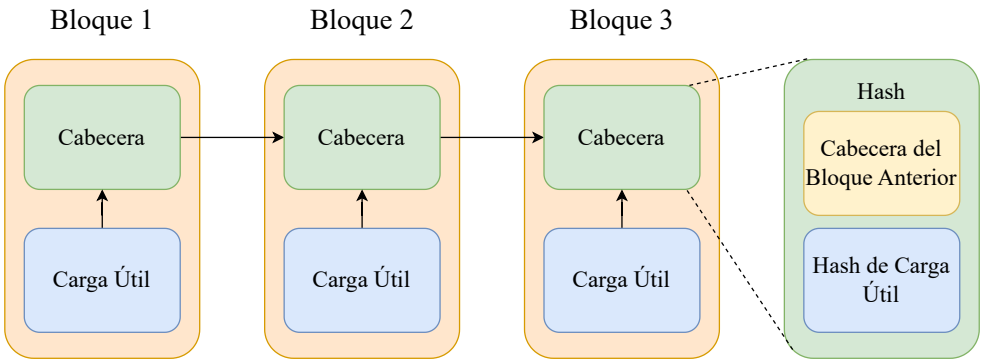


Figura 3.8: Método genérico de encadenamiento de bloques.

Tipos de Blockchain

Las blockchains pueden clasificarse en mayoritariamente en tres categorías principales: públicas, privadas y de consorcio. Cada tipo tiene características y aplicaciones específicas que se adaptan a diferentes necesidades y casos de uso en el contexto de la tecnología y la industria. Blockchain Pública: Las blockchains públicas son redes completamente descentralizadas en las que cualquiera puede unirse y participar. No existe una autoridad central que controle la red, lo que garantiza un alto nivel de transparencia y resistencia a la censura. Todas las

transacciones y datos almacenados en una blockchain pública son accesibles para cualquier persona, permitiendo auditar y verificar de manera independiente todas las operaciones. Este tipo de blockchain es ideal para aplicaciones que requieren total transparencia y descentralización, como las criptomonedas (e.g., Bitcoin [85] y Ethereum [88]). Las blockchains públicas utilizan mecanismos de consenso como Proof of Work (PoW) o Proof of Stake (PoS) para asegurar la red y validar las transacciones. Sin embargo, estos mecanismos de consenso son una de las principales críticas a la blockchain debido a la cantidad de recursos computacionales que utilizan. El consumo energético de estos mecanismos, como en el caso de Bitcoin, puede llegar a ser mayor que el consumo anual de energía de países enteros como Chile [86, 87]. Las blockchains públicas enfrentan algunas amenazas conocidas:

- **Ataques del 51 %:** Este ataque ocurre cuando un actor malintencionado o un grupo de actores controla más del 50 % de la potencia de hashing (en blockchains que usan Proof of Work) o de las monedas en stake (en blockchains que usan Proof of Stake). Con este control mayoritario, los atacantes pueden manipular la blockchain para doble gastar, revertir transacciones confirmadas o bloquear nuevas transacciones.

- **Ataques de Carrera (Race Attacks):** Ocurren cuando un atacante intenta realizar dos transacciones conflictivas al mismo tiempo, con la esperanza de que una se confirme antes que la otra, permitiendo el doble gasto. Estos ataques explotan la velocidad de la red y el tiempo de confirmación de las transacciones.

- **Ataques de Eclipse:** Un ataque de eclipse ocurre cuando un nodo de la blockchain es aislado y rodeado por nodos controlados por el atacante. El atacante puede manipular la visión del nodo aislado sobre la blockchain, retrasando o censurando transacciones específicas.

Blockchain Privada: En contraste, las blockchains privadas están restringidas a un grupo específico de participantes autorizados. Una entidad central o un consorcio de entidades controla la red, decidiendo quién puede leer y escribir en la blockchain. Esta estructura proporciona mayor privacidad y permite un rendimiento más alto, ya que el número de nodos es limitado y el consenso puede ser alcanzado más rápidamente. Las blockchains privadas son adecuadas para aplicaciones empresariales que requieren control sobre el acceso a los datos y alta eficiencia operativa. Ejemplos destacados de plataformas de blockchain privadas incluyen Hyperledger Fabric [89] y Corda [90], que se utilizan en industrias como la banca, la gestión de la cadena de suministro y el sector gubernamental.

Las principales amenazas a las blockchains privadas son:

- **Amenazas Internas:** Como el riesgo de colusión, donde un grupo de participantes con acceso autorizado podría coludirse para manipular las transacciones o influir en el proceso de consenso. La colusión puede socavar la integridad y la confiabilidad de la red.

- **Vulnerabilidades Externas:** Debido a su centralización, un único punto encargado del procesamiento y almacenamiento es más vulnerable a ataques en comparación con varios puntos distribuidos.

Blockchain de Consorcio: Las blockchains de consorcio combinan características de las blockchains públicas y privadas. En una blockchain de consorcio, un grupo de organizaciones colabora para mantener la red y compartir el control sobre el proceso de consenso. Solo las entidades autorizadas pueden unirse y participar en la red, proporcionando un equilibrio entre transparencia, control y eficiencia. Las blockchains de consorcio son particularmente útiles en contextos donde varias entidades necesitan trabajar juntas de manera confiable y segura, como en el sector energético, la banca y la atención médica. Ejemplos de blockchains de consorcio incluyen Quorum [91] y R3 Corda [92].

Las amenazas principales a las blockchains de consorcio incluyen:

- **Riesgos de Colusión:** Similar a las blockchains privadas, donde los miembros del consorcio pueden coludirse para manipular el proceso de consenso.
- **Ataques de Denegación de Servicio (DoS):** Que pueden interrumpir el servicio y la disponibilidad de la red, afectando la colaboración entre las entidades del consorcio.

Tabla 3.4: Comparación de Tipos de Blockchain.

Tipo	Descripción	Pros	Contras	Amenazas	Ref.
Pública	Red descentralizada abierta a todos donde cualquiera puede participar y validar transacciones.	Alta transparencia y resistencia a la censura; Alta seguridad a través de consenso distribuido.	Baja eficiencia y escalabilidad; Alto consumo energético; Baja privacidad.	Ataques del 51 %, ataques de carrera, ataques de eclipse.	[87]
Privada	Red controlada por una entidad o un grupo selecto, con acceso restringido a participantes autorizados.	Alta eficiencia y rendimiento; Alta privacidad y control sobre los datos.	Menor transparencia; Riesgo de colusión; Vulnerabilidades en un punto central de control.	Amenazas internas, vulnerabilidades externas.	[89], [90]
Consorcio	Red administrada por un grupo de organizaciones que comparten el control y el proceso de consenso.	Equilibrio entre transparencia y privacidad; Alta eficiencia y rendimiento; Control compartido reduce riesgos individuales.	Riesgo de colusión entre miembros; Complejidad en la gestión y gobernanza.	Riesgos de colusión, ataques de denegación de servicio (DoS).	[91], [92]

3.5. Vulnerabilidades

En el ámbito de eHealth, existen múltiples vectores de ataque que representan serios riesgos para la seguridad y privacidad de los datos de los pacientes. Uno de los principales vectores de ataque es la falta de esquemas criptográficos robustos en la transmisión y almacenamiento de datos médicos sensibles, lo que puede permitir interceptaciones no autorizadas y accesos indebidos. Aunque muchos sistemas actuales emplean algoritmos de criptografía robustos, un gran porcentaje de estos están mal implementados. En el estudio [93] se concluye que muchos errores en la implementación de la criptografía se deben a una combinación de falta de conocimiento, uso inapropiado de bibliotecas criptográficas y prácticas inseguras de manejo de claves. Este artículo destaca la necesidad de un enfoque más sistemático para la educación, pruebas y verificación de software criptográfico para evitar vulnerabilidades críticas en el futuro.

Además, muchos dispositivos médicos conectados a redes IoMT presentan deficientes mecanismos de seguridad, facilitando ataques como la suplantación de identidad, acceso remoto

no autorizado, denegación de servicio, ataques de canal lateral e inyección de fallas. La implementación inadecuada de actualizaciones de seguridad y parches también expone a los sistemas eHealth a exploits y malware, aumentando la superficie de ataque. La interoperabilidad entre diferentes sistemas de salud, aunque esencial para el intercambio eficiente de información, puede introducir puntos débiles si no se manejan adecuadamente las políticas de seguridad y privacidad. Asimismo, la dependencia en infraestructuras de nube y fog computing introduce riesgos adicionales, como la posibilidad de ataques de denegación de servicio (DoS) que pueden interrumpir servicios críticos.

Por último, la falta de capacitación y concienciación en ciberseguridad entre los profesionales de la salud puede llevar a prácticas inseguras, como el uso de contraseñas débiles o la compartición inadecuada de credenciales, exacerbando las vulnerabilidades del sistema. Estas vulnerabilidades subrayan la necesidad de un enfoque integral y proactivo en la seguridad de eHealth, abarcando desde la implementación de tecnologías avanzadas de criptografía hasta la formación continua del personal sanitario.

3.5.1. Criptoanálisis

El criptoanálisis es la disciplina que se enfoca en estudiar y romper sistemas criptográficos con el objetivo de encontrar debilidades y vulnerabilidades en ellos. Este campo implica el análisis de algoritmos de cifrado y descifrado para descubrir cómo se pueden comprometer sin conocer la clave secreta utilizada. Los criptoanálisis utilizan diversas técnicas matemáticas, estadísticas y de ingeniería inversa para intentar descifrar mensajes cifrados, evaluar la seguridad de los sistemas criptográficos y proponer mejoras para hacerlos más resistentes a los ataques. En resumen, el criptoanálisis es fundamental para garantizar la seguridad y robustez de los métodos criptográficos empleados para proteger la información [94]. Un área que ha tenido mucho auge en los último años es el criptoanálisis en sistemas embebidos. Existe una variedad de ataques conocidos como ataques de hardware que rompen cifrados robustos analíticamente. Por otro lado, el criptoanálisis convencional busca encontrar errores en los algoritmos de cifrado, encontrando debilidades para explotar. A continuación se abordan ambos enfoques.

Seguridad de Hardware

La seguridad del hardware, realiza ataques de implementación que logran romper algoritmos criptográficos seguros y violar sistemas de seguridad en tiempos récord. Estos ataques se introdujeron por primera vez en [95], logrando romper RSA, Diffie-Hellman y otros sistemas mediante un análisis del tiempo que toma la ejecución del algoritmo. A partir de este punto, se desarrollaron una serie de ataques de implementación que resultan ser particularmente efectivos en dispositivos con recursos limitados. Entre estos ataques, los más populares son el análisis de canal lateral (SCA) [96] y los ataques de inyección de fallos (FI, Fault Injection) [97]. SCA puede explotar cualquier información que se filtre a través del hardware. Los SCAs más comunes son los ataques de temporización, que aprovechan las variaciones en los tiempos de ejecución de diferentes operaciones [95], los ataques de energía que utilizan los cambios en el consumo de energía en el hardware para vulnerar algoritmos criptográficos [98], y los ataques de radiación que explotan las diferencias en las emisiones electromagnéticas del hardware durante el procesamiento de información [99]. Por otro lado, los ataques de FI

más populares incluyen FI de voltaje, que interrumpe el suministro de voltaje durante un intervalo de tiempo predeterminado [9], FI de reloj que modifica selectivamente uno de los períodos del reloj [100], y FI a través de pulsos electromagnéticos cerca del dispositivo bajo ataque [101]. Todos estos ataques son difíciles de abordar ya que explotan vulnerabilidades en la implementación del cifrado en el hardware y no solo el cifrado en sí. El alcance de estos ataques es sumamente amplio y una contramedida global solo puede ser realizada por hardware como se explica en [98]. Sin embargo existen modificaciones de software que permiten abordar la mayoría de ataques al menos dificultándolos. Muchas de estas modificaciones están implementadas en librerías como ECClibs [70] por lo que seleccionar algún algoritmo que cuente con contramedidas implementadas es muy importante. Por otro lado, la nueva generación de algoritmos de criptografía ligera como Ascon [61] son resistentes a muchos ataques de hardware.

Criptoanálisis Clásico

Los ataques de criptoanálisis típicos que no son dirigidos al hardware se centran en debilidades inherentes en los algoritmos criptográficos y en sus fundamentos matemáticos. Entre ellos, los ataques de texto claro conocido (Known-plaintext attacks) son comunes; aquí, el atacante tiene acceso tanto al texto cifrado como al texto en claro correspondiente, lo que le permite intentar deducir la clave o el algoritmo utilizado. Los ataques de texto cifrado elegido (Chosen-plaintext attacks) permiten al atacante seleccionar textos en claro específicos y obtener sus correspondientes textos cifrados, proporcionando información útil para deducir la clave. Los ataques de texto cifrado conocido (Ciphertext-only attacks) son más difíciles, ya que el atacante solo tiene acceso a textos cifrados y debe intentar descifrar la clave o el texto en claro sin información adicional [102].

Además, los ataques de texto cifrado elegido (Chosen-ciphertext attacks) son otra técnica donde el atacante puede elegir textos cifrados y obtener los textos en claro correspondientes, ayudando a identificar debilidades en el algoritmo de descifrado. Los ataques de clave relacionada (Related-key attacks) utilizan varias claves relacionadas de una manera conocida para intentar descubrir la clave maestra o el algoritmo de cifrado. Los ataques de fuerza bruta (Brute force attacks) implican probar todas las combinaciones posibles de claves hasta encontrar la correcta, aunque este método es muy costoso en términos de tiempo y recursos. Por último, el criptoanálisis diferencial y el criptoanálisis lineal son técnicas avanzadas que analizan cómo las diferencias en los textos en claro afectan las diferencias en los textos cifrados y utilizan aproximaciones lineales al comportamiento del cifrado, respectivamente, para encontrar relaciones que puedan revelar información sobre la clave. Estos métodos destacan por su enfoque en la debilidad del algoritmo y no en las implementaciones del hardware [102].

3.5.2. Ataques de Denegación de Servicio

Los ataques de Denegación de Servicio (DoS, Denial-of-Service) son una variante de ataque, en donde un usuario malicioso tiene por objetivo impactar los recursos de un sistema. Consecuentemente, la disponibilidad de los recursos del sistema son mermados, impactando la confiablidad, seguridad y resiliencia brindada a los usuarios legítimos. Habitualmente, en un ataque del tipo DoS, el atacante genera una abrumadora cantidad de datos para agotar los recursos del sistema, y con ello degradar el desempeño del sistema. Es altamente proba-

ble que el atacante sea capaz de interrumpir por completo el funcionamiento del sistema y denegar el acceso a los usuarios legítimos.

El atacante tiene una serie de estrategias para generar un DoS en el sistema y continuamente han estado evolucionando. Dentro de las estrategias DoS más analizadas en la literatura científica, se encuentran: ataques de inundación de tráfico, ataques de agotamiento de recursos, ataques de suplantación, ataques de interrupción de servicio y ataques de agotamiento de energía. Recientemente en la comunidad ha sido de especial interés una novedosa estrategia DoS, denominada Denegación de Servicio Distribuidos (DDoS), en redes IoT [103, 104].

En el contexto de las estrategias DDoS y sus diferentes enfoques, los ataques del tipo jamming son especialmente destructivos [105] . El jamming es una estrategia de ataque, en donde el usuario malicioso interfiere intencionalmente con la comunicación inalámbrica entre los usuarios legítimos del sistema. Mediante la generación de señales de interferencia en la banda de frecuencia de las comunicaciones legítimas, el atacante tiene el potencial de denegar las comunicaciones. Desde el punto de vista del atacante, el iniciar este tipo de ataques presenta baja complejidad y un alto grado de éxito en denegar los recursos, en especial en redes narrow band [106].

Por ello, los ataques del tipo jamming en sistemas eHealth son potencialmente peligrosos, al exponer información vital de trabajadores y pacientes y con ello, su integridad, salud y seguridad. A consecuencia de esto, es de vital importancia el desarrollo de estrategias de defensa robustas que garanticen la disponibilidad e integridad de las comunicaciones.

3.5.3. Ataques de Escucha o Interceptación (Eavesdropping or Sniffing Attacks)

El concepto de interceptación de comunicaciones fue introducido por primera vez en 1949 por Claude Shannon, quien planteó el problema del Canal de Secretos en su trabajo seminal [107]. Según este concepto, la capacidad del atacante para recuperar la señal interceptada depende de la relación señal-ruido (SNR) recibida. Si la SNR es suficientemente alta, el atacante puede recuperar con éxito la señal y, por ende, los datos transmitidos.

Los ataques de escucha o interceptación, también conocidos como ataques de sniffing, son una amenaza significativa en el ámbito de las comunicaciones seguras, especialmente en redes IoT. Estos ataques implican la interceptación y lectura de datos sensibles que se están transmitiendo a través de un canal de comunicación. Un atacante que emplea técnicas de escucha puede capturar información confidencial, como credenciales de usuario, datos personales y comunicaciones privadas, sin que los usuarios legítimos sean conscientes de esta actividad maliciosa.

El uso de cifrado de extremo a extremo es una medida para proteger los datos de los usuarios legítimos durante la transmisión. También, la autenticación mutua entre dispositivos para asegurar que solo los nodos autorizados puedan comunicarse, y el monitoreo continuo de la red para detectar y responder a actividades sospechosas son medidas que mitigan estos ataques. Además, el empleo de técnicas de enmascaramiento de datos y el cambio frecuente de canales de comunicación dificultan significativamente la capacidad del atacante

para interceptar y decodificar las transmisiones.

Estudios recientes han explorado diversas estrategias para fortalecer la seguridad contra ataques de escucha en redes IoT. En [108] se revisan enfoques basados en aprendizaje automático para mejorar la detección y mitigación de ataques en sistemas IoT. Por otro lado, en la investigación [109] analizan los bloques de construcción y las interacciones de componentes en arquitecturas IoT, destacando la importancia de implementar medidas de seguridad en cada capa de la arquitectura para proteger contra ataques de escucha.

3.5.4. Ataques de Suplantación de Identidad (Spoofing Attacks)

En el ámbito del Internet de las Cosas (IoT), los ataques de suplantación de identidad representan una amenaza significativa para la seguridad y la integridad de las redes y dispositivos conectados. Estos ataques ocurren cuando un atacante se hace pasar por un dispositivo legítimo al falsificar datos de identificación como direcciones IP, direcciones MAC o credenciales de autenticación, engañando así a otros dispositivos y sistemas para obtener acceso no autorizado.

En las redes IoT, la suplantación de direcciones IP es particularmente peligrosa. Un atacante puede modificar la dirección IP de los paquetes que envía para aparentar provenir de un dispositivo confiable dentro de la red. Este tipo de suplantación puede permitir al atacante acceder a recursos restringidos, realizar ataques de denegación de servicio (DoS) o incluso tomar el control de dispositivos IoT para crear una botnet. La suplantación de direcciones MAC, donde el atacante altera la dirección de hardware de su dispositivo, puede ser utilizada para eludir filtros de seguridad basados en direcciones MAC, permitiendo el acceso a redes privadas [110, 111].

Los ataques de suplantación en IoT no se limitan a la manipulación de direcciones. Los atacantes también pueden falsificar mensajes de comunicación, engañando a los dispositivos para que acepten comandos maliciosos. Esto es especialmente crítico en sistemas IoT que controlan infraestructura vital, como sistemas de salud, redes eléctricas o vehículos autónomos, donde la ejecución de comandos falsificados puede tener consecuencias desastrosas [112].

Para mitigar los riesgos de los ataques de suplantación de identidad en IoT, es fundamental implementar medidas de seguridad robustas. Esto incluye el uso de autenticación mutua entre dispositivos, cifrado de comunicaciones y el monitoreo continuo de las redes para detectar comportamientos anómalos. Además, el despliegue de protocolos de seguridad como IPSec y el uso de certificaciones digitales puede ayudar a asegurar que solo los dispositivos legítimos puedan comunicarse entre sí [110, 111].

Capítulo 4

Algoritmos y Esquemas Propuestos

En este capítulo, se presenta el modelo del sistema y se desarrolla y explica el esquema criptográfico propuesto que garantiza la seguridad de la información, así como los esquemas de comunicación que aseguran una transmisión confiable en la segunda arquitectura (arquitectura LPWAN), la cual utiliza dispositivos comunicados con tecnologías de largo alcance, como se explicó en el capítulo 2.

Inicialmente, se explica el modelo del sistema para luego presentar el esquema de comunicación de referencia y las partes involucradas en el esquema criptográfico. A continuación, se detalla tanto la construcción de los esquemas de transmisión como el esquema criptográfico involucrado en los dispositivos IoMT. Este enfoque integral asegura que los datos transmitidos sean seguros y que las comunicaciones sean fiables, abarcando desde la transmisión hasta la recepción y validación de la información.

4.1. Modelo del Sistema

Esta investigación se centra en la seguridad y confiabilidad de la comunicación entre dispositivos de recursos limitados pertenecientes a un usuario y una estación base (BS). Los dispositivos se comunican a través de canales inalámbricos con la BS utilizando tecnología LPWAN. Por otro lado, la BS se conecta mediante un enlace confiable con los centros de salud, los cuales forman parte de una red blockchain. Cada centro de salud actúa como un nodo de esta red, siendo responsable del esquema criptográfico y del almacenamiento de la base de datos distribuida en cada nodo. Para representar una estructura eHealth más completa y realista, se considera que los centros de salud interactúan con la nube, la cual añade inteligencia y otras funciones a la información que reciben o generan los centros de salud.

En este trabajo, no se analiza en detalle el enlace entre la BS, los centros de salud, la red blockchain ni la nube; se asume que estos enlaces son completamente confiables y funcionales. No obstante, se proponen lineamientos sobre la criptografía que deben manejar para garantizar la seguridad de la información a lo largo de toda la arquitectura. Además, no se profundizará en el enlace ascendente de los dispositivos, pero se considera que el análisis

es análogo al enlace descendente.

Asimismo, se asume que el canal de enlace descendente entre la BS y los dispositivos IoT está sujeto a desvanecimiento de Rayleigh cuasi-estático y puede operar bajo diferentes tasas de transmisión. La probabilidad de interrupción del enlace de cada esquema de transmisión se puede calcular evaluando la expresión de la ecuación (3.5), considerando el R_s de cada esquema y la ganancia del canal $g = \kappa \mathrm{d}^{-\alpha}$, donde κ es una constante dependiente de la frecuencia, d es la distancia entre el dispositivo y la BS, y α es el exponente de pérdida de trayecto quedando la ecuación 4.1 [47].

$$P_{\text{out}} = 1 - \exp\left(-\frac{N_o W(2^{\frac{R_s}{W}} - 1)}{P_t \kappa \mathrm{d}^{-\alpha}}\right). \tag{4.1}$$

4.1.1. Esquema de Comunicación de Referencia

El esquema típico de comunicación entre la estación base (BS) y los clientes ligeros es la transmisión directa (DT), en la cual la BS envía un bloque de datos y un encabezado para cada ronda de transmisión. Las firmas y los bloques se transmiten de forma independiente, lo que significa que ambos pueden ser transmitidos exitosamente, se puede perder uno de ellos o incluso ambos. Por lo tanto, la interrupción de la información en un esquema de transmisión ($\mathcal{O}\mathrm{I}^{\mathrm{sch}}$) ocurre por la unión de dos eventos independientes: la pérdida irrecuperable de un bloque de datos o la imposibilidad de validación del bloque, debido a la pérdida de las firmas necesarias para su validación.

Sin perder generalidad, consideramos que cada bloque y firma contienen l bits, respectivamente, y que deben ser transmitidos en un intervalo de tiempo igual a τ, lo que lleva a una tasa de transmisión $R_s = 2l/\tau$. Además, asumimos que la probabilidad de perder un bloque es igual a la de perder una firma, denotando con p la probabilidad de perder un mensaje de tamaño l. En el esquema DT, perder un bloque de datos o una firma implica un evento de interrupción de la información. Por lo tanto, la probabilidad de interrupción de la información se puede escribir como:

$$\mathcal{O}\mathrm{I}^{\mathrm{DT}} = 2p - p^2. \tag{4.2}$$

4.1.2. Esquemas de Transmisión

En el ámbito de las comunicaciones inalámbricas, la confiabilidad de la transmisión de datos es un aspecto crítico, especialmente cuando se trata de dispositivos IoT de baja potencia utilizados en el área de la salud (IoMT). Los esquemas de transmisión convencionales pueden no ser suficientes para garantizar que los datos se reciban íntegramente y sin interrupciones. Por esta razón, es necesario considerar estrategias adicionales que aumenten la confiabilidad de las transmisiones.

Una de estas estrategias es la incorporación de redundancia a través de la repetición o codificación de los datos. La redundancia permite que, incluso si una parte de los datos se pierde durante la transmisión, haya suficiente información adicional para recuperar los datos originales. Sin embargo, la adición de redundancia debe hacerse de manera eficiente, respetando los recursos limitados disponibles para cada ronda de transmisión. Esto implica

que tanto la información original como la redundante deben utilizar la misma cantidad de recursos, equivalente a un intervalo de tiempo τ.

En este contexto, la tasa de transmisión R_s debe ajustarse según el número de paquetes redundantes añadidos. Por ejemplo, si un esquema de transmisión utiliza b bloques de datos y s firmas en una ronda, la tasa de transmisión resultante será $R_s = (b + s)l/\tau$.

La evaluación de los diferentes esquemas de transmisión se basa en su probabilidad de interrupción de la información $\mathcal{O}\mathrm{I}^{\mathrm{sch}}$. Esta probabilidad combina dos eventos distintos: la pérdida irreversible de un bloque, denominada probabilidad de interrupción de bloque ($O\mathrm{b}$), y la probabilidad de interrupción de firma (O_{s}). Estas probabilidades son diferentes de la simple probabilidad de perder un bloque o una firma, ya que pueden incluir el efecto de recuperar bloques o firmas perdidos mediante réplicas o mensajes codificados transmitidos en otras rondas.

Para limitar la complejidad del análisis, consideramos solo cuatro rondas consecutivas. Esta restricción ayuda a gestionar eficientemente los recursos de decodificación, evitando el aumento de costos en términos de tiempo y consumo de energía, especialmente en dispositivos de baja potencia. Con estos fundamentos, los esquemas basados en repetición o codificación que se discuten a continuación permiten calcular la probabilidad de interrupción de la información de la siguiente manera:

$$\mathcal{O}\mathrm{I}^{\mathrm{sch}} = O\mathrm{s} + O_{\mathrm{b}} - O_{\mathrm{s}}O_{\mathrm{b}}. \tag{4.3}$$

Como los bloques y las firmas se transmiten de forma independiente, primero discutimos estrategias para aumentar la confiabilidad de los bloques. Además, dado que una ronda de transmisión (compuesta por bloque y firma) se recibe sin su firma, aún puede considerarse válida si una de las rondas subsecuentes se recibe con su firma respectiva, nos enfocamos principalmente en métodos para aumentar la confiabilidad de la transmisión de los bloques.

Esquemas de Repetición

Los esquemas de repetición repiten un mensaje un cierto número de veces, para aumentar la probabilidad de que algunas de las réplicas lleguen exitosamente. Para este tipo de esquema de transmisión, el enlace falla solo cuando se pierden todas las réplicas de un bloque. Esto significa que la probabilidad de perder irreversiblemente un bloque depende del número de repeticiones b y de la probabilidad de interrupción de la transmisión de un bloque

$$O_{\mathrm{b}} = p^b. \tag{4.4}$$

Esquemas Codificados

Los esquemas codificados hacen uso de mensajes codificados para aumentar la confiabilidad del enlace. Para mantener el proceso de decodificación lo más simple posible, consideramos que cada mensaje codificado contiene la información de solo dos bloques diferentes. Esto se logra a través de una relación lógica entre los mensajes, como la operación XOR. O_{b} debe calcularse para cada esquema codificado y no existe una ecuación genérica para describirlo.

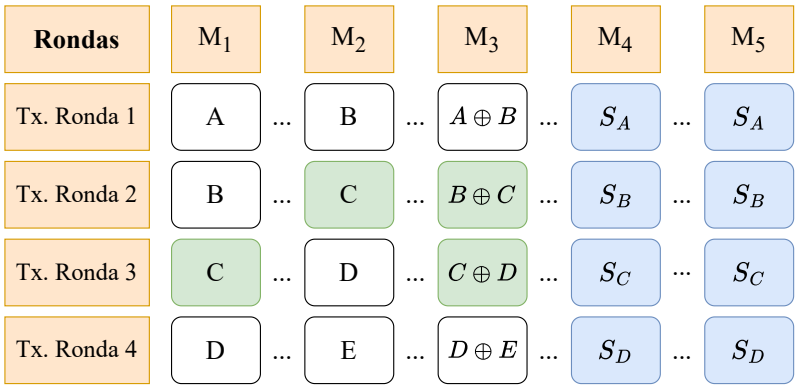


Figura 4.1: Representación de cuatro rondas de transmisión y su contenido para un esquema de transmisión codificado de mensajes de bloques.

Para comprender mejor cómo se definen estas probabilidades, supongamos que estamos en medio de una transmisión donde la estructura de la ronda está compuesta por dos bloques con información diferente y un bloque codificado. Luego, nos referimos a M_1 como el primer bloque (enviado primero en la ronda anterior), M_2 como el segundo bloque (enviado por primera vez en la ronda actual), y M_3 como el mensaje codificado (de los dos bloques enviados en la ronda actual), como se muestra en la Figura 4.1. Los mensajes de una sesión de comunicación se entrelazan con otros mensajes para espaciarse al menos un tiempo de coherencia del canal.

La recuperación de información de bloques codificados es factible bajo ciertas condiciones. Siempre que uno de los bloques y el bloque codificado estén disponibles, se puede recuperar la información. Por ejemplo, considere un escenario donde la información recibida es B, y el bloque codificado contiene información sobre A y B. Si no recibimos un bloque con información A, aún podemos recuperar la información A utilizando el bloque B recibido y el bloque codificado. Para determinar la probabilidad de interrupción de bloque, denotada como O_b, considere, por ejemplo, la información representada por C en la Figura 4.1. Luego, enumerando todos los eventos de pérdida de C, O_b se puede calcular como [45]

$$O_\mathrm{b} = p^4 + 4p^6 - 6p^7 + 6p^8 - 12p^9 + 13p^{10} - 6p^{11} + p^{12}, \tag{4.5}$$

que se puede aproximar bien como

$$O_\mathrm{b} \approx p^4 + 4p^6. \tag{4.6}$$

Note que las ecuaciones anteriores solo son válidas para el caso de dos bloques de datos y un mensaje codificado que combine estos dos bloques. Si se consideran más bloques de datos o más mensajes codificados, entonces la probabilidad de interrupción de la información debe calcularse nuevamente según los principios anteriores.

Probabilidad de Interrupción de Firma

Cada firma se transmite de forma independiente y puede recuperarse utilizando el mecanismo de "amortización de firmas". Por lo tanto, solo consideramos el uso de la replicación

Tabla 4.1: Resumen de los esquemas de transmisión.

Esquema	**Tasa de Transmisión**	O_{b}	O_{s}	$\mathcal{O}_{\mathrm{I}}^{\mathrm{sch}}$
DT	34 kbps	p	p	$2p - p^2$
RT 201	51 kbps	p^2	p^4	$p^2 + p^4$
CT 111	51 kbps	$p^3 + 3p^4$	p^4	$p^3 + 4p^4$
RT 301	68 kbps	p^3	p^4	$p^3 + p^4$
CT 211	68 kbps	$p^4 + 4p^6$	p^4	$2p^4 + 4p^6$
CT 121r	68 kbps	$p^4 + 2p^5$	p^4	$2p^4 + 2p^5$
CT 121d	68 kbps	$3p^5 + 3p^7$	p^4	$p^4 + 3p^5$
RT 302	85 kbps	p^3	p^8	$p^3 + p^8$
RT 401	85 kbps	p^4	p^4	$2p^4 - p^8$
CT 212	85 kbps	$p^4 + 4p^6$	p^8	$p^4 + 4p^6$
CT 122r	85 kbps	$p^4 + 2p^5$	p^8	$p^4 + 2p^5$
CT 122d	85 kbps	$3p^5 + 3p^7$	p^8	$3p^5 + 3p^7$
RT 402	102 kbps	p^4	p^8	$p^4 + p^8$
CT 222r	102 kbps	$p^6 + 2p^7$	p^8	$p^6 + 2p^7$
CT 222d	102 kbps	$p^6 + 12p^9$	p^8	$p^6 + p^8$
CT 132r	102 kbps	$p^5 + p^6$	p^8	$p^5 + p^6$
CT 132d	102 kbps	$p^6 + 4p^7$	p^8	$p^6 + 4p^7$

para aumentar su confiabilidad, de modo que

$$O_{\mathrm{s}} = p^s, \tag{4.7}$$

donde s es el número de firmas dentro de cuatro rondas consecutivas, dentro de las cuales limitaremos el proceso de recuperación por simplicidad de implementación en el dispositivo. Así, la propiedad de "amortización de firmas" se limita a cuatro rondas.

Comparación de esquemas de transmisión

Esta sección resume los esquemas de transmisión considerados en este artículo. La Tabla 4.1 enumera los nombres de los esquemas, su tasa de transmisión, O_{b}, O_{s}, y su probabilidad de interrupción de la información $\mathcal{O}_{\mathrm{I}}^{\mathrm{sch}}$. El nombre del esquema se interpreta de la siguiente manera: "CT 212" significa *"Transmisión Codificada con 2 bloques de datos, 1 bloque codificado, y 2 firmas"* y después de los dígitos, puede haber una "r" (repetido) o "d" (diferente) que se refiere a si los bloques codificados son los mismos o codifican la información de dos maneras diferentes. La probabilidad de interrupción de la información considera solo los dos términos más relevantes.

4.1.3. Esquema Criptográfico

El esquema criptográfico propuesto se diseñó utilizando algoritmos seleccionados tras una exhaustiva revisión bibliográfica, con el objetivo de implementarlos en todos los dispositivos de la capa de sensores. Estos dispositivos, como se detalla en el capítulo 3, suelen tener

recursos limitados, por lo que los algoritmos de seguridad implementados deben ser computacionalmente eficientes, pero capaces de mantener un alto nivel de seguridad (equivalente a 128 bits). Para los algoritmos criptográficos seleccionados, se realizaron pruebas comparativas cuyos resultados se presentan en el capítulo 5. Además, se proponen algoritmos criptográficos para el resto de la arquitectura; sin embargo, estos carecen de pruebas empíricas sobre su desempeño y fueron seleccionados únicamente basándose en la bibliografía existente. Las pruebas empíricas de los algoritmos utilizados en las capas de borde y nube se dejan como trabajo futuro.

Los dispositivos de recursos limitados, como los IoMT utilizados en el ámbito de la salud, requieren un bajo uso de memoria RAM y flash, además de un consumo energético reducido [10]. Las métricas como la velocidad y el tiempo de cifrado no son tan prioritarias, ya que la mayoría de los algoritmos de cifrado operan dentro de un rango de tiempo aceptable. Si un algoritmo no cumple con este criterio, es probable que también presente un alto consumo energético.

En cuanto a la seguridad de la información, los dispositivos IoMT deben garantizar la autenticación durante la comunicación y proteger la confidencialidad e integridad de los datos, siguiendo el nivel 2 de seguridad definido por la norma IEEE 802.15.6 [10]. El esquema de seguridad también debe ser capaz de mitigar o dificultar ataques de hardware, ataques de denegación de servicio (DoS), interceptación de datos y suplantación de identidad. A continuación, se presenta el flujo de la información en la arquitectura estudiada y los procesos involucrados:

Los dispositivos de recursos limitados (IoMT o wearables) generan un intercambio de claves a través de una estación base con la red blockchain. Uno o más nodos de la red blockchain realizan este intercambio de claves con el dispositivo, le asigna un identificador y lo asocia al usuario al que pertenece el dispositivo. Ahora, el dispositivo cuenta con una clave simétrica conocida por los centros de salud, un ID y un usuario asociado. El usuario y el ID se utilizan para crear credenciales en las aplicaciones que sean necesarias para trabajar con la información generada por el dispositivo o para enviarle información.

Flujo de Información en Dos Casos Hipotéticos

Para entender el flujo de información, consideraremos dos casos hipotéticos: el primero donde se desea enviar información al dispositivo y el segundo donde el dispositivo quiere enviar información.

Primer caso: Envío de información al dispositivo

Supongamos que desde los registros en la nube de un determinado usuario se identifica que su dispositivo requiere una actualización de firmware debido a una vulnerabilidad a cierto ataque. Para esto, se procede a enviar la información necesaria al centro de salud utilizando un método seguro de transmisión para dispositivos de altas prestaciones computacionales. Una vez que el centro de salud cuenta con la información correspondiente, la envía a través de una estación base, cifrando los datos con Ascon-128a. El tag generado por Ascon en el bloque anterior, un identificador del dispositivo y una marca de tiempo se añaden a los datos asociados del siguiente bloque. Para el primer bloque, solo se necesita agregar el identificador

del dispositivo y la marca de tiempo. En el lado del dispositivo de recursos limitados, la información se autentica y descifra con Ascon, descartando los tags a medida que se obtiene nueva información autenticada hasta completar el archivo necesario.

Segundo caso: Envío de información desde el dispositivo

Un dispositivo de recursos limitados desea enviar información a una aplicación en la nube. Para esto, cifra la información con Ascon-128a, encadenando la información actual con el tag del bloque anterior, el identificador del nodo blockchain al que se envía la información y una marca de tiempo. Esta información se envía a la estación base, que la transmite al centro de salud correspondiente al nodo blockchain destinatario del mensaje. En el centro de salud, la información se autentica, verifica y descifra. Luego, se identifica que el dispositivo está asociado a alguna aplicación en la nube y se procede a enviar la información utilizando un método de transmisión seguro para dispositivos de altos recursos computacionales. Esta información se procesa en la nube y se devuelve al centro de salud en una forma más "digerida".

Registro de Transacciones en la Red Blockchain

Para registrar las transacciones de información de los usuarios en la red blockchain, toda la información procesada se agrega al registro distribuido de la blockchain. Los centros de salud agrupan las transacciones recibidas en un intervalo de tiempo determinado de forma sincrónica. Una vez que todos los centros tienen la información que desean agregar, se envía a la red para ser añadida a la base de datos distribuida mediante un mecanismo de consenso. En la red blockchain, cada nodo representa un centro de salud que realiza intercambios de claves seguros con los dispositivos de los usuarios y almacena una copia actualizada de la base de datos distribuida. Para agregar bloques, los nodos validan el próximo bloque mediante consenso. Los bloques contienen transacciones procesadas en la nube, cada una asociada al usuario que la emite. Se realiza una firma agregada de todas las transacciones y del bloque anterior utilizando firmas agregadas BLS, que permiten verificar la participación de un usuario sin conocer otras firmas o credenciales. La única información pública necesaria para identificar la información de un usuario serán las firmas agregadas en las que esté involucrado, y la verificación de estas firmas BLS confirma la presencia del usuario en el bloque correspondiente [83].

Partes involucradas y criptografía correspondiente

- **Dispositivos de Bajo Consumo y Usuarios**: Generan el intercambio de claves seguro utilizando secp256r1, cifran la información garantizando su confidencialidad, autenticidad e integridad con Ascon-128a, y envían/reciben datos a través de la estación base.

- **Estación Base (BS)**: Actúa como intermediario para la transmisión de datos entre los dispositivos de bajo consumo y los centros de salud.

- **Centros de Salud**: Representan un nodo de la blockchain, realizan los intercambios de claves seguros con los dispositivos, autentican, verifican y descifran la información recibida con Ascon-128a. Interactúan tanto con la nube como con la red blockchain, y se comunican con los dispositivos de recursos limitados a través de la estación base.

Utilizan protocolos de comunicación altamente seguros como SSH, HTTPS y TLS para conectarse con la nube.

- **Red Blockchain**: Almacena una copia actualizada de la base de datos distribuida en cada uno de sus nodos, realiza el consenso para agregar nuevos bloques y asegura la integridad y autenticidad de las transacciones mediante firmas agregadas BLS.

- **Nube**: Proporciona procesamiento adicional y agrega inteligencia a la información, facilitando la toma de decisiones y el análisis de datos, y retransmite la información procesada a los centros de salud. Utiliza protocolos de comunicación altamente seguros como SSH, HTTPS y TLS.

El esquema descrito es mostrado en la Figura 4.2 donde k_{AB} es la clave compartida mediante ECDH, $\xi_{k_{AB}(P_N)}$ es el criptograma de un cifrado simétrico utilizando la clave k_{AB} y evaluando el texto en claro P_N, T_N es el Tag generado por el cifrado simétrico, V es el proceso de verificación de un Tag y D el proceso de descifrado.

Encadenamiento de la información con Ascon-128a

Como se mencionó en el capítulo 2, Ascon tiene la capacidad de asociar datos, los cuales pueden ser validados a través del tag que genera Ascon. El proceso de encadenamiento de información con Ascon-128a, representado en la Figura 4.3, se utiliza para garantizar que cualquier alteración en un bloque de datos sea detectable en el siguiente bloque. Este mecanismo es esencial en sistemas que requieren altos niveles de seguridad e integridad, como las redes blockchain en entornos de salud.

Se observa que el proceso de encadenamiento genera bloques de texto cifrado de 128 bits y tags de 128 bits. Los tags una vez utilizados pueden ir siendo desechados para ahorrar espacio a excepción del último que sirve para ir encadenando información adicional. A continuación, se describe el flujo del proceso:

1. **Cifrado del Primer Bloque**

   - Se utiliza el texto en claro P_0, junto con una marca de tiempo inicial y el ID del nodo blockchain.

   - Ascon-128a cifra el texto en claro y genera un tag T_0.

2. **Cifrado de Bloques Subsiguientes**

   - Cada bloque subsiguiente usa el tag del bloque anterior como parte de sus datos asociados.

   - Se añade también una nueva marca de tiempo y el ID del nodo blockchain.

   - Este proceso asegura que cualquier alteración en un bloque previo invalide la autenticidad de los bloques subsiguientes.

3. **Verificación y Autenticación**

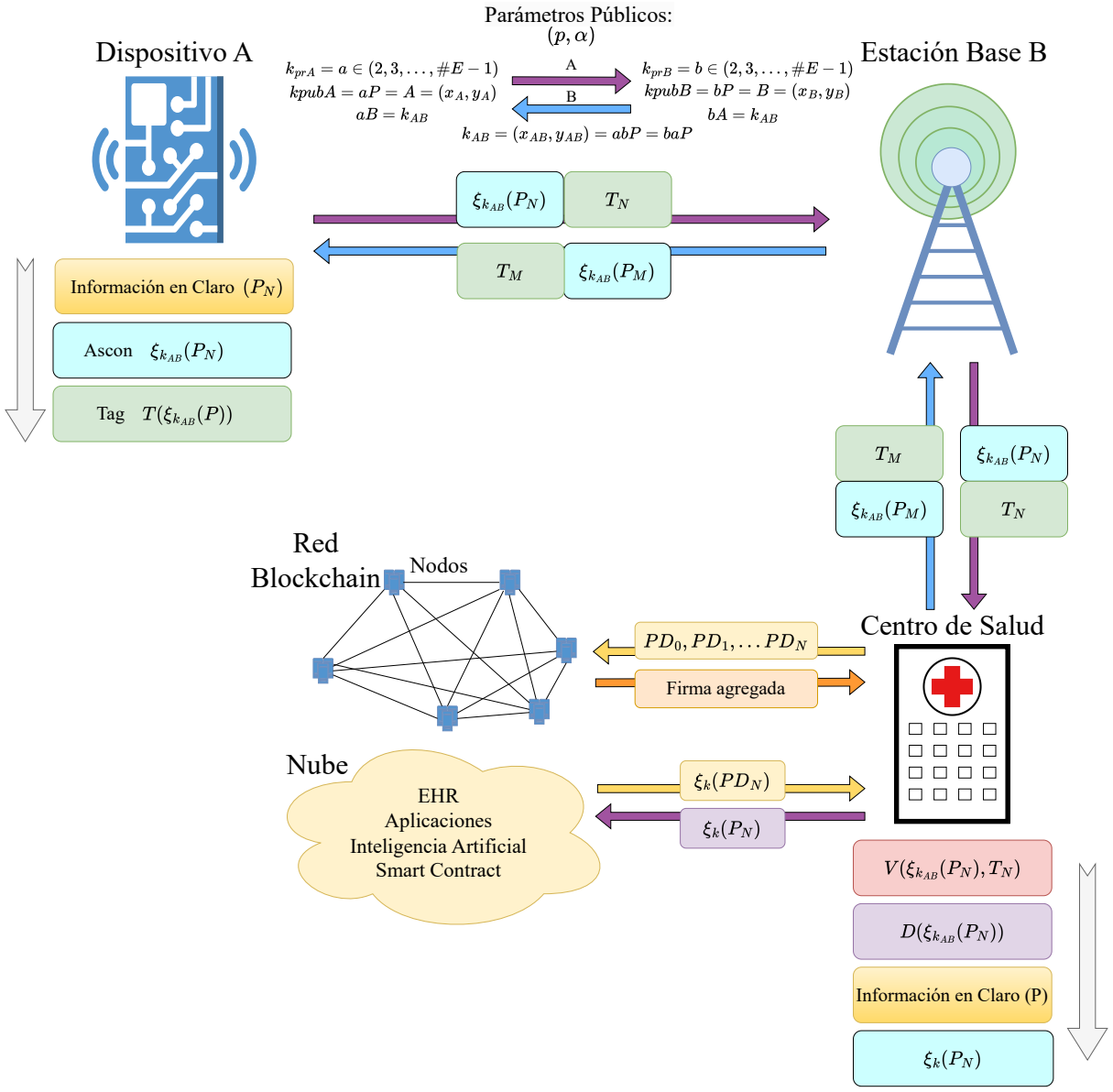


Figura 4.2: Esquema criptográfico propuesto para la arquitectura con dispositivos de recursos limitados de largo alcance utilizando Ascon-128a y secp256r1.

- El dispositivo receptor puede verificar cada bloque cifrado mediante el tag.
- Si algún bloque ha sido alterado, el proceso de autenticación fallará, asegurando que solo la información íntegra y auténtica sea aceptada.

Por lo tanto, podemos ver como cada bloque de texto cifrado de 128 bits queda asociado de forma inequívoca a un ID y un marca de tiempo gracias al Tag de 128 bits. De esta forma no solo se garantiza la seguridad y la integridad de los datos, sino que también facilita la auditoría y el seguimiento de transacciones en sistemas distribuidos, proporcionando una base robusta para la gestión de información crítica en entornos de recursos limitados. Cabe destacar que existe la posibilidad de incluir un marca de tiempo en el nonce puede ser útil

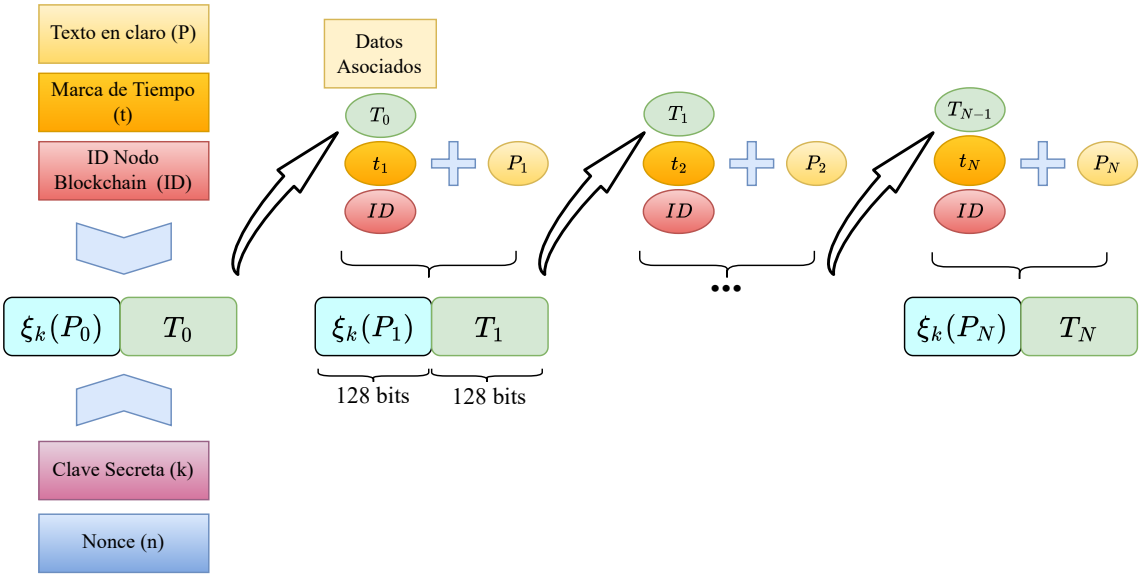


Figura 4.3: Proceso de encadenamiento de bloques utilizando Ascon-128a.

para garantizar que el nonce es único si no hay otra fuente de unicidad (como un contador o un valor aleatorio). Por último, de ahora en adelante en vez de el termino Tag nos referiremos a este como Firma ya que cumple con las características de seguridad necesarias: Representa de forma inequívoca la información, no se puede generar a partir del texto cifrado y queda asociada al dispositivo (por lo tanto a un usuario) a través de la clave compartida.

Capítulo 5

Resultados y Discusión

En este capítulo, se presentan y analizan los resultados obtenidos de la evaluación de varios esquemas de transmisión y algoritmos criptográficos en arquitecturas LPWAN para eHealth. La evaluación de los esquemas de transmisión se realizó mediante simulaciones, utilizando los parámetros de NB-IoT, con el objetivo de determinar la cobertura máxima antes de que ocurra una interrupción en la comunicación desde la estación base hasta los dispositivos de recursos limitados. Por otro lado, la parte experimental se enfoca en la implementación y evaluación de los algoritmos criptográficos seleccionados en dispositivos de recursos limitados, midiendo el consumo de memoria flash, RAM, y los ciclos de reloj. Además, se estimaron los recursos de memoria necesarios para la codificación y decodificación de los mensajes. Finalmente, se analiza la robustez de los algoritmos frente a diversos escenarios de ataque. Los resultados combinan simulaciones y pruebas experimentales, proporcionando una visión integral de la eficacia y viabilidad de las propuestas en entornos reales de eHealth.

5.1. Esquemas de Transmisión

Comparamos el rendimiento de varios esquemas basados en repeticiones y transmisiones codificadas. El análisis considera la probabilidad de interrupción de la información y asume los parámetros mostrados en la Tabla 5.1. Estos valores son típicos de la tecnología IoT de banda estrecha basada en tecnología celular (NB-IoT) [33] y de los algoritmos criptográficos seleccionados para esta aplicación.

La primera simulación se realizó para observar el impacto de la tasa de transmisión en la probabilidad de interrupción del enlace. Cabe destacar que la probabilidad de interrupción del enlace es igual a la probabilidad de pérdida de información si la información transmitida no tiene sobrecarga o redundancia añadida. Los resultados de esta simulación se muestran en la Figura 5.1.

La sección de color coral claro en el gráfico delimita toda la región donde la probabilidad de interrupción del enlace supera 0.1. Este valor es el umbral máximo para la pérdida de información en la tecnología NB-IoT [33]. En consecuencia, cualquier probabilidad de pérdida de información que supere este umbral resulta en una interrupción de la comunicación.

Tabla 5.1: Parámetros utilizados para las simulaciones.

Parámetro	**Valor**	**Referencia**
Ancho de banda (W)	180 kHz	[113], [114]
Exponente de pérdida de trayecto (α)	2.78	[39]
Constante de frecuencia (κ)	$7 \cdot 10^{-4}$ (902 MHz)	[45]
Tasa de transmisión (R_s)	68 - 226.7 kbps	[33]
Máxima interrupción tolerada	0.1	[33]
Intervalo de tiempo (τ)	7.5 ms	
Bloques de recursos NB-IoT	1260	
Longitud del bloque	128 bits	
Longitud de la firma	128 bits	
Radio de cobertura máximo	20 km	[32]
Potencia de transmisión	23 dBm	[113], [114], [115]
Ruido normalizado	-174 dBm/Hz	[33]

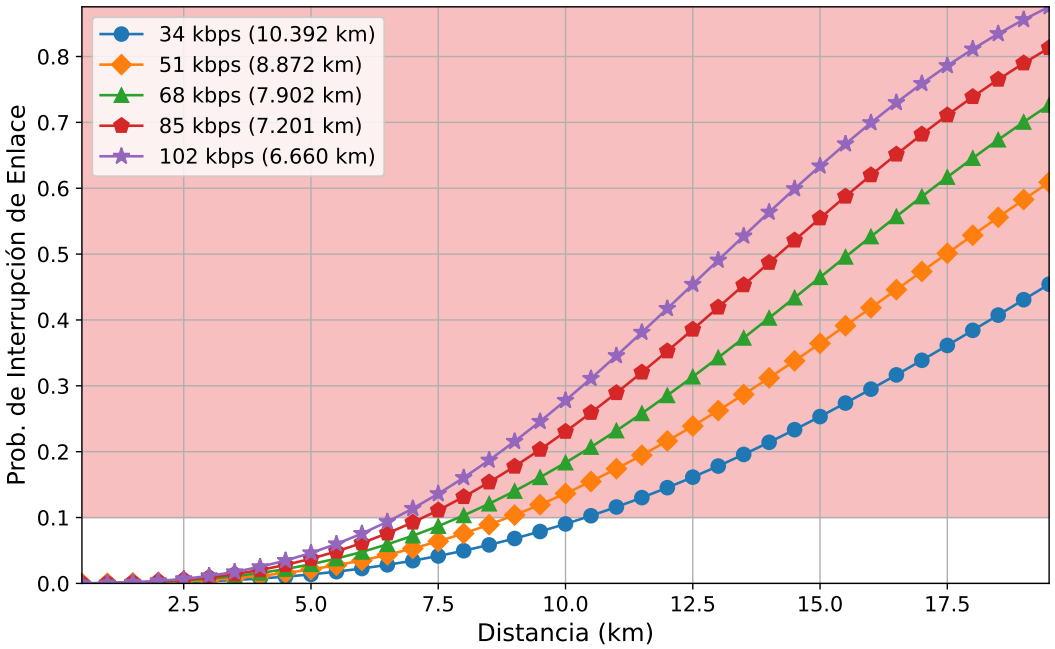


Figura 5.1: Probabilidad de outage vs distancia para distintas tasas de transmisión

Además, la distancia a la cual cada tasa de transmisión alcanza este umbral se muestra en la leyenda del gráfico. Los resultados demuestran que la probabilidad de interrupción del enlace aumenta con tasas de transmisión más altas y a medida que la distancia incrementa.

A continuación, para verificar la precisión de las expresiones analíticas calculadas para cada esquema de transmisión, realizamos una simulación de Monte Carlo. En la simulación, utilizamos 10 iteraciones por punto y las promediamos. Estas simulaciones son temporal y computacionalmente costosas, especialmente para las codificaciones más robustas. Por lo tanto, todas las simulaciones se realizaron para valores altos de probabilidad de interrupción ($> 10^{-2}$). Sin embargo, elegimos para cada tasa de transmisión un esquema a ser simulado hasta una probabilidad de interrupción más baja (10^{-2}) como se muestra en la Figura 5.2, lo

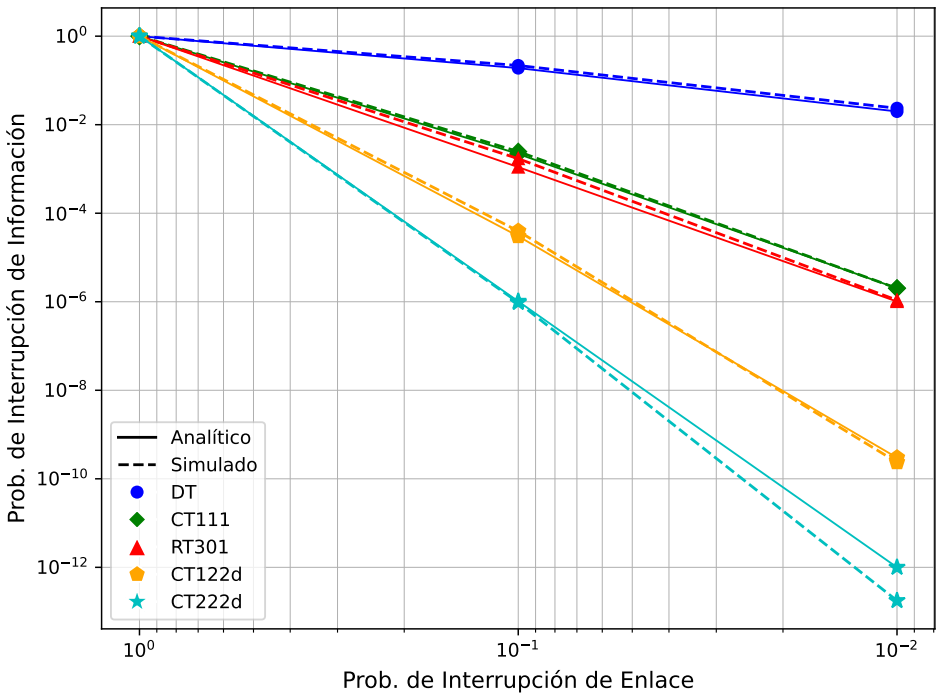


Figura 5.2: Simulación Monte Carlo para validar los esquemas propuestos.

cual tomó aproximadamente 3 semanas. El tiempo de ejecución de las simulaciones de Monte Carlo aumenta exponencialmente a medida que disminuye la probabilidad de interrupción, extendiéndose más allá de varios meses para calcular probabilidades de 10^{-3}. El resultado se muestra en la Figura 5.2, donde se observa un excelente acuerdo entre los resultados de la simulación y los modelos analíticos. Los modelos analíticos se validaron con un nivel de significancia de $\alpha = 0{,}05$. A partir de ahora, nos basamos exclusivamente en las aproximaciones proporcionadas en la Tabla 4.1 para el siguiente análisis.

Luego, la Figura 5.3 muestra la comparación de tres esquemas en términos de probabilidad de interrupción de la información: DT, con una tasa de transmisión de 34 kbps, y dos con tasas de 51 kbps, etiquetadas como RT201 y CT111. Se puede observar que CT111 tiene un mejor rendimiento para todas las distancias bajo el umbral determinado por NB-IoT, alcanzando una cobertura máxima de $\sim$16.1 km. Además, se observa que RT201 y CT111 mejoran considerablemente la cobertura para tasas de transmisión de 51 kbps. Finalmente, hay una reducción notable en la cobertura para DT en comparación con una tasa de transmisión de 34 kbps. Esto se debe a que DT carece de cualquier forma de redundancia; solo agrega una firma para garantizar la autenticación del mensaje.

Además, la Figura 5.4 presenta los resultados obtenidos considerando esquemas de transmisión con una tasa de 68 kbps. El esquema CT121d muestra el mejor rendimiento, alcanzando una cobertura de casi 15 km. Sin embargo, todos los esquemas logran una cobertura similar de alrededor de $\sim$14.5 km. Es notable que RT301 demuestra un fuerte rendimiento con un enfoque sencillo para agregar redundancia, lo que podría ser un factor crucial depen-

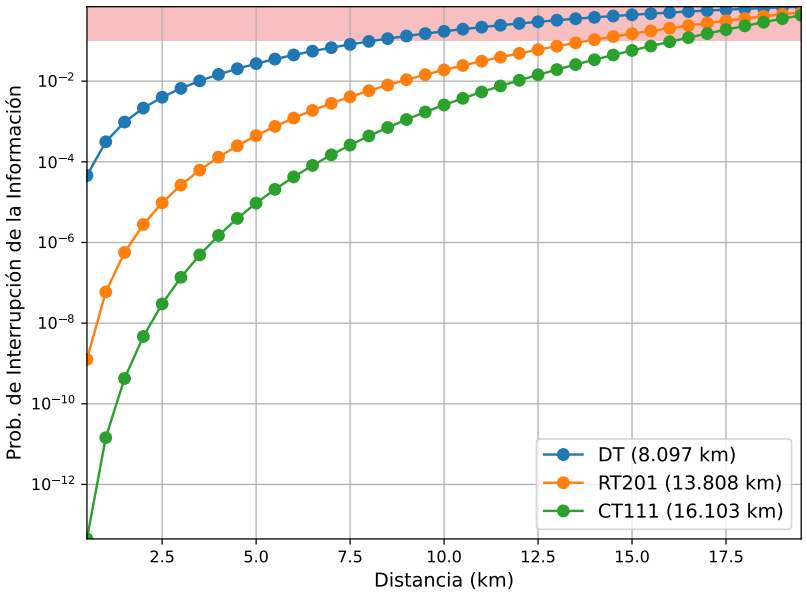


Figura 5.3: Probabilidad de interrupción de la información vs distancia para esquemas con tasas de transmisión de 34 kbps y 51 kbps.

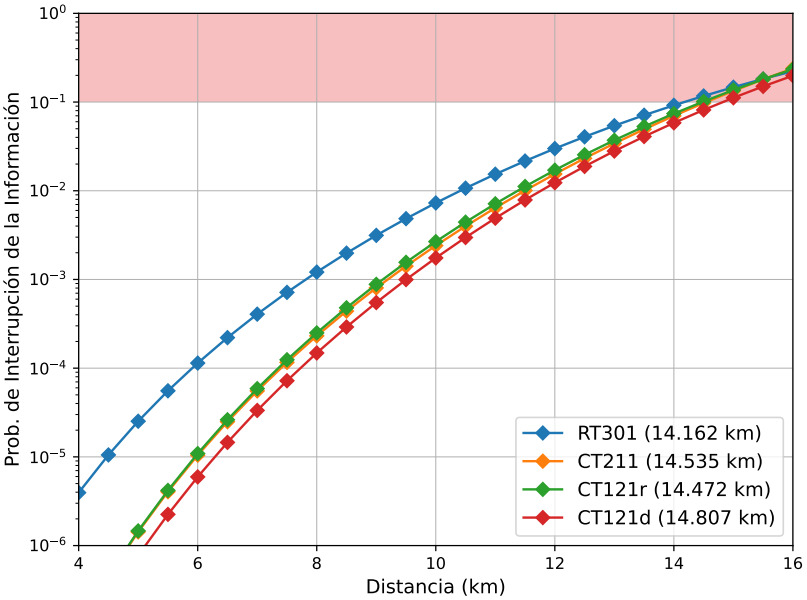


Figura 5.4: Probabilidad de interrupción de la información vs distancia para esquemas con una velocidad de transmisión de 68 kbps.

diendo de los recursos del dispositivo, ya que los esquemas de repetición son menos exigentes computacionalmente.

A continuación, se presentan los resultados de los esquemas de transmisión con tasas de 85 kbps en la Figura 5.5. Se puede observar que el esquema CT122d presenta el mejor rendimiento. Además, se observa que agregar redundancia a la firma disminuye el rendimiento del esquema de repetición RT302, resultando en una cobertura reducida en comparación con RT301, como se presenta en la Figura 5.4. Además, aumentar las repeticiones, como

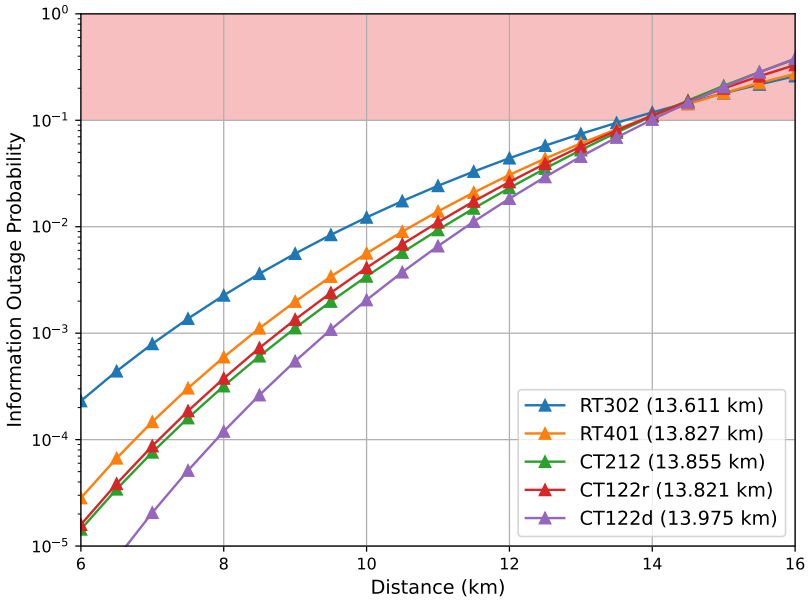


Figura 5.5: Probabilidad de interrupción de la información vs distancia para esquemas con una velocidad de transmisión de 85 kbps.

en RT401, conduce a una peor cobertura. A partir de esto, se puede inferir que entre los esquemas de repetición, RT301 es el que mejor rendimiento presenta. Esto coincide con el óptimo identificado para alta densidad de nodos en [40], donde se analizaron exhaustivamente los esquemas de repetición.

En la Figura 5.6, se presentan los resultados para esquemas con tasas de transmisión de 102 kbps. A esta tasa de transmisión, el esquema CT222d supera a todos los demás, logrando una cobertura máxima de ∼15.1 km. Cabe señalar que estos esquemas, excepto RT402, son ligeramente más complejos de implementar en comparación con los de tasas de transmisión más bajas.

Los mejores esquemas para cada tasa de transmisión se muestran en la Figura 5.7. El primer gráfico presenta los resultados de la simulación, mientras que el segundo gráfico proporciona una vista ampliada de la región donde los esquemas se cruzan. En la subfigura superior, se observa que el esquema CT111 supera a los demás en términos de cobertura máxima, alcanzando aproximadamente ∼16.1 km. Sin embargo, en la subfigura inferior, se puede ver que el esquema CT222d tiene una mejor probabilidad de interrupción que los otros esquemas para distancias menores a ∼13.3 km. Aunque CT222d ofrece una ventaja en distancias más cortas, CT111 sigue siendo una opción preferible en la mayoría de los casos debido a su mayor cobertura y simplicidad de implementación.

La Tabla 5.2 presenta un resumen de la cobertura máxima de los esquemas de transmisión estudiados. Las filas coloreadas de marrón claro corresponden a la cobertura alcanzada sin un esquema de transmisión para diferentes tasas de transmisión. Por otro lado, las filas coloreadas de verde claro corresponden a los esquemas CT111, RT201 y CT222d. Estos esquemas son el que tiene la mejor cobertura, el que tiene la mejor cobertura para esquemas de repetición y el mejor esquema en términos de probabilidad de interrupción de la información a menos

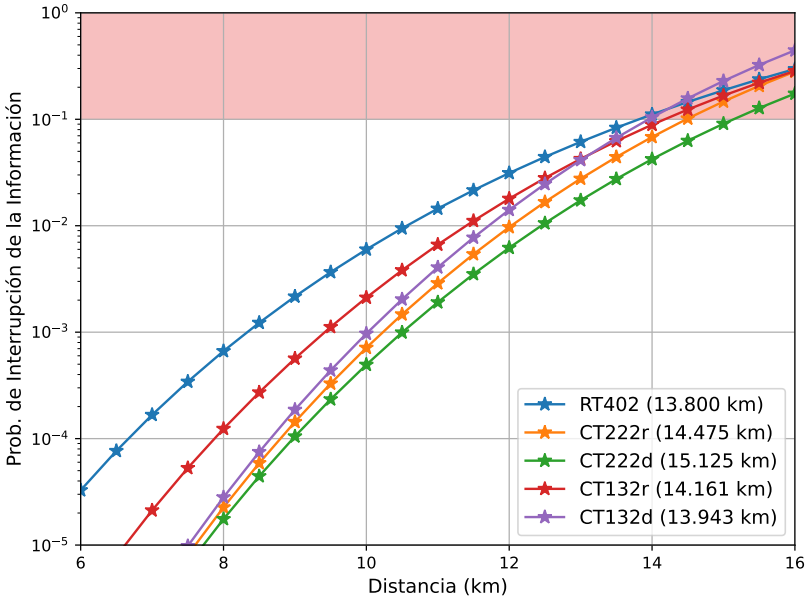


Figura 5.6: Probabilidad de interrupción de la información vs distancia para esquemas con una velocidad de transmisión de 102 kbps.

de 13.3 km.

Cabe destacar que, aunque los esquemas CT111 y CT222d utilizan dos tipos de codificación ligeramente diferentes, CT222d tiene la posibilidad de codificar la misma información de dos maneras diferentes. Esto añade complejidad computacional (que, aunque es baja, debe ser considerada) para el dispositivo de decodificación. En nuestra opinión, CT111 representa una mejor opción en la mayoría de los casos, ya que no solo logra una mayor cobertura, sino que también es más sencillo.

Finalmente, para analizar el rendimiento de los esquemas bajo diferentes condiciones de la red, estos se evaluaron utilizando un modelo de desvanecimiento Nakagami-m, considerando tres valores de m, incluyendo Rayleigh como caso especial. La Figura 5.8 muestra la probabilidad de interrupción de la información en función de la distancia entre el RCD y la BS para los esquemas más destacados en diversos modelos de canal.

Las dos subfiguras en la parte superior ilustran la equivalencia entre el modelo Rayleigh y el Nakagami-m cuando m=1, mientras que el aumento en los componentes de línea de vista (equivalente al aumento en m) provoca una disminución en la probabilidad de interrupción de la información, como era de esperarse. Es importante notar que la tendencia de los esquemas se mantiene, pero sin duda, la relación entre los esquemas en función de la distancia varía. Por lo tanto, la toma de decisiones sobre qué esquema utilizar para cada RCD también depende de sus condiciones de línea de vista con respecto a la BS.

Las Tablas 5.3 y 5.4 presentan las probabilidades de interrupción de la información de los esquemas más destacados para diferentes valores de $m = 1, 2, 4$ a distancias de 5 y 10 km, respectivamente. Como era de esperar, el aumento de los componentes de línea de vista (equivalente al aumento de m) causa una disminución en la probabilidad de interrupción de

Tabla 5.2: Resumen de la cobertura máxima de los esquemas de transmisión.

Esq. de Tx.	**Tasa de Tx. [kbps]**	**Máx. Cobertura [km]**
-	34	10.392
DT	34	8.097
-	51	8.872
RT 201	51	13.808
CT 111	51	16.103
-	68	7.902
RT 301	68	14.162
CT 211	68	14.535
CT 121r	68	14.472
CT 121d	68	14.807
-	85	7.201
RT 302	85	13.611
RT 401	85	13.827
CT 212	85	13.855
CT 122r	85	13.821
CT 122d	85	13.975
-	102	6.660
RT 402	102	13.800
CT 222r	102	14.475
CT 222d	102	15.125
CT 132r	102	14.161
CT 132d	102	13.943

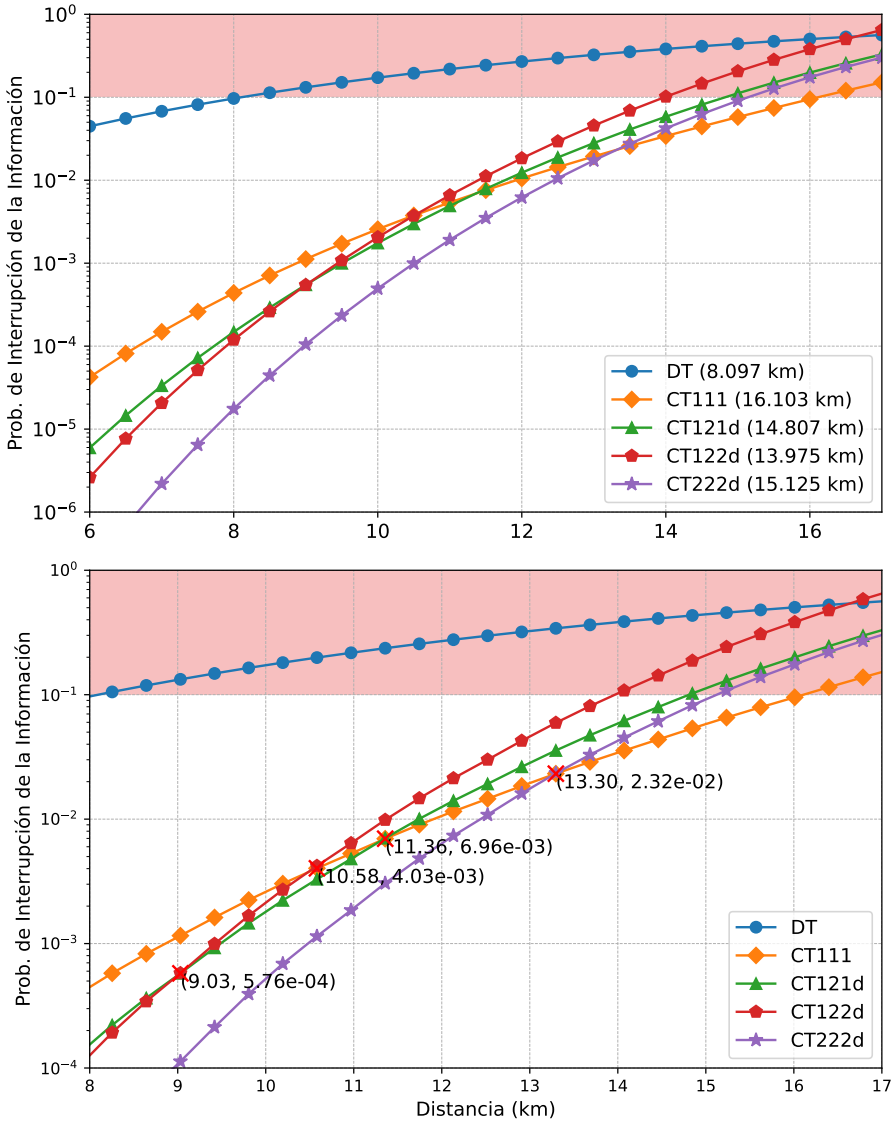


Figura 5.7: Probabilidad de interrupción de la información vs distancia para los mejores esquemas de transmisión en cada velocidad de transmisión (34, 51, 68, 85 y 102 kbps). (a) La subfigura superior muestra los resultados, destacando la cobertura máxima. (b) La subfigura inferior muestra una ampliación de la anterior, resaltando las intersecciones entre los esquemas.

la información. Cabe destacar que la tendencia de los esquemas se mantiene, pero sin duda, la relación entre los esquemas en función de la distancia varía. Por lo tanto, la elección del esquema a utilizar para cada RCD también depende de sus condiciones de línea de vista con respecto a la BS.

Tabla 5.3: Probabilidad de interrupción de la información de los esquemas más destacados para $m = \{1, 2, 4\}$ a una distancia de 5 km.

Esquema	**Parámetro** m		
	1	**2**	**4**
DT	$2{,}72 \cdot 10^{-2}$	$7{,}45 \cdot 10^{-4}$	$7{,}33 \cdot 10^{-7}$
CT111	$9{,}44 \cdot 10^{-6}$	$6{,}90 \cdot 10^{-10}$	$1{,}35 \cdot 10^{-17}$
CT121d	$7{,}72 \cdot 10^{-7}$	$7{,}59 \cdot 10^{-12}$	$-3{,}65 \cdot 10^{-19}$
CT122d	$2{,}19 \cdot 10^{-7}$	$4{,}76 \cdot 10^{-13}$	$-3{,}90 \cdot 10^{-18}$
CT222d	$9{,}71 \cdot 10^{-9}$	$7{,}28 \cdot 10^{-15}$	$-4{,}19 \cdot 10^{-18}$

Tabla 5.4: Probabilidad de interrupción de la información de los esquemas más destacados para $m = \{1, 2, 4\}$ a una distancia de 10 km.

Esquema	**Parámetro** m		
	1	**2**	**4**
DT	$1{,}72 \cdot 10^{-1}$	$3{,}13 \cdot 10^{-2}$	$1{,}26 \cdot 10^{-3}$
CT111	$2{,}57 \cdot 10^{-3}$	$4{,}48 \cdot 10^{-5}$	$2{,}98 \cdot 10^{-8}$
CT121d	$1{,}75 \cdot 10^{-3}$	$1{,}85 \cdot 10^{-5}$	$8{,}10 \cdot 10^{-9}$
CT122d	$2{,}05 \cdot 10^{-3}$	$2{,}66 \cdot 10^{-5}$	$1{,}53 \cdot 10^{-8}$
CT222d	$4{,}94 \cdot 10^{-4}$	$7{,}27 \cdot 10^{-6}$	$6{,}47 \cdot 10^{-9}$

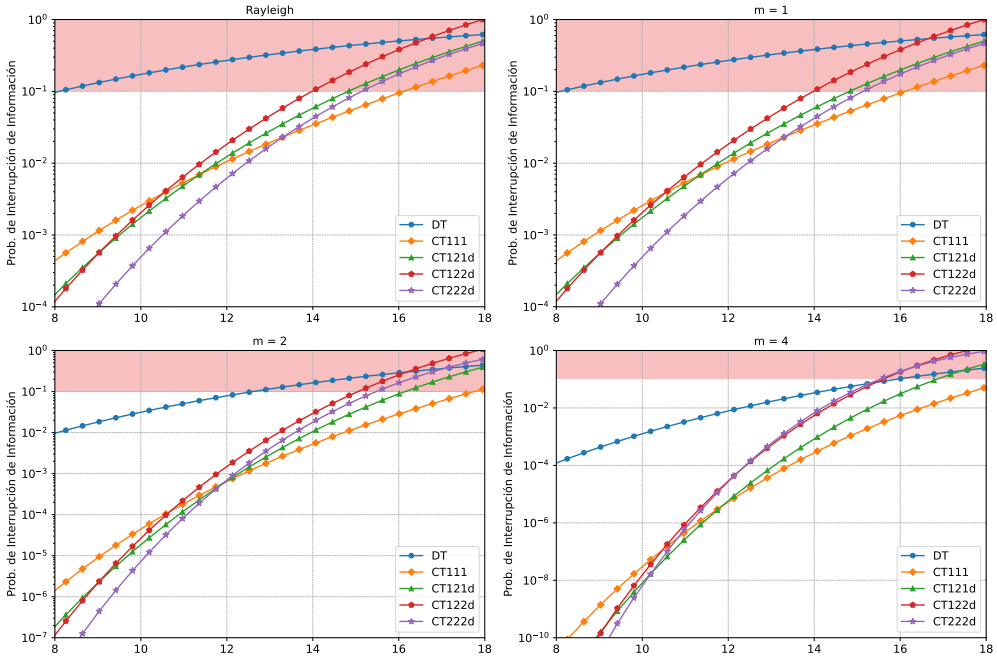


Figura 5.8: Probabilidad de interrupción de información en función de la distancia entre RCD y BS, para los esquemas más destacados para diferentes modelos de canales, modelo de desvanecimiento de Rayleigh (arriba a la izquierda) y Nakagami-m con $m = 1$ (arriba a la derecha), $m = 2$ (abajo a la izquierda) y $m = 4$ (abajo a la derecha).

5.2. Evaluación de Recursos

5.2.1. Comparación de Algoritmos Criptográficos

Se compararon los algoritmos propuestos en [8] con algoritmos criptográficos que, basados en nuestra revisión bibliográfica, parecían prometedores para su implementación en dispositivos de recursos limitados. Las métricas de comparación incluyeron los ciclos de reloj necesarios para ejecutar el algoritmo, la memoria flash y la memoria RAM requeridas. Los algoritmos simétricos evaluados fueron AES-128 y Ascon-128a. Los algoritmos asimétricos comparados fueron las curvas secp256r1 y Curve25519 para el intercambio de llaves Diffie-Hellman. Aunque en nuestra propuesta prescindimos de utilizar un hash para firmar y utilizamos el Tag proporcionado por Ascon, también se evaluaron los hashes Blake2s y Ascon-Hash.

Los resultados obtenidos en el modulo ESP32 WROOM-32D se presentan en la Tabla 5.5, donde se destacan en verde claro las filas de los algoritmos seleccionados para nuestro esquema criptográfico. Se observa que Ascon-128a supera ampliamente a AES-128 en términos de ciclos de reloj y memoria requerida. Para los algoritmos de hash, también se aprecia una diferencia significativa en la memoria requerida, aunque no tanto en los ciclos de reloj. En cuanto a la criptografía asimétrica, se confirma que Curve25519 es más rápida, como se menciona en [71–73]. Sin embargo, esta curva requiere una cantidad considerablemente mayor de memoria. Dado que el intercambio de llaves se realizará con poca frecuencia, preferimos la curva secp256r1 sobre Curve25519, ya que nos deja más memoria flash libre para otros usos en dispositivos de recursos limitados.

Tabla 5.5: Comparación de algoritmos criptográficos en el ESP32.

Algoritmo	**Ciclos de reloj**	**Flash [bytes]**	**RAM [bytes]**
AES-128 cifrado	32,566	278,972	7,984
AES-128 descifrado	25,380	278,972	7,984
Ascon-128a cifrado	19,519	31,784	376
Ascon-128a descifrado	8,649	31,784	376
ECDH 25519	15,465,098	39,176	664
ECDH secp256r1	22,942,395	34,004	384
Blake2s	16,208	38,688	688
Ascon-Hash	15,660	30,920	376

Por otro lado, los resultados obtenidos en el microcontrolador ATMEGA328P se presentan en la Tabla 5.6, donde se destacan en verde claro las filas de los algoritmos seleccionados para nuestro esquema criptográfico. Se observa que Ascon-128a supera, pero no ampliamente a AES-128 en términos de ciclos de reloj y memoria requerida a diferencia de lo que ocurría con la implementación en el modulo ESP32. Para los algoritmos de hash, la diferencia es más clara ya que la diferencia en memoria flash es más del doble y para los ciclos de reloj es casi el triple, quedando como claro ganador Ascon-Hash. En cuanto a la criptografía asimétrica, Curve25519 se mantiene ligeramente más rápida. Sin embargo, a diferencia de los resultados obtenidos con la ESP32 la curva25519 muestra un mejor uso más eficiente de la memoria flash pero no de la RAM. Para este dispositivo no es tan clara la elección entre curvas, pero nos mantendremos con la curva secp256r1 ya que es más fácil de implementar y las implementaciones poseen contramedidas para ataques de canal lateral ampliamente

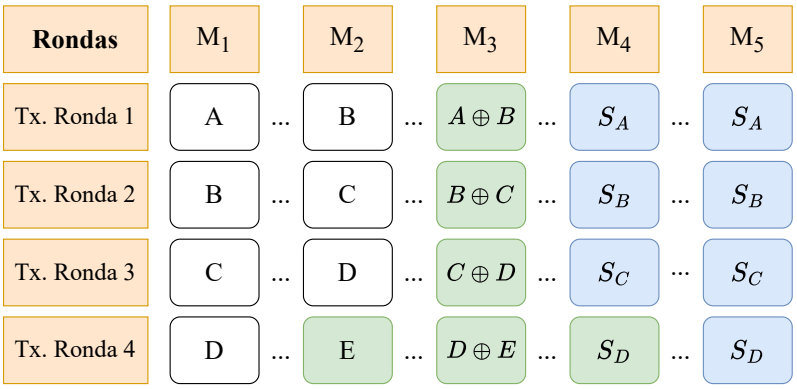


Figura 5.9: Escenario del peor caso para el uso de RAM (los bloques verdes representan los bloques de datos y la firma recibida).

avaladas.

Tabla 5.6: Comparación de algoritmos criptográficos en el ATMEGA328P.

Algoritmo	**Ciclos de reloj**	**Flash [bytes]**	**RAM [bytes]**
AES 128 cifrado	21,056	4,530	553
AES 128 descifrado	17,344	4,530	553
Ascon 128a cifrado	12,502	3,728	227
Ascon 128a descifrado	12,508	3,728	227
ECDH 25519	60,186,944	5,456	862
ECDH secp256r1	68,710,592	7,824	545
Blake2s	57,024	7,952	609
Ascon-Hash	22,030	3,448	576

5.2.2. Estimación de Memoria para el Esquema Propuesto

Inicialmente se calculan los recursos necesarios para la codificación de bloques para el peor escenario. El peor escenario se considera cuando se han recibido los bloques y las firmas necesarias para recuperar y validar la cadena de bloques justo antes de que se considere una interrupción de la información. En este escenario, se reciben cuatro bloques codificados y un bloque normal, los cuales ocuparán una cantidad fija de memoria hasta que la información del bloque D sea validada o ocurra una interrupción. Para validar estos bloques, se comienza con el bloque E y el bloque codificado $D \oplus E$. Se decodifica el bloque D y se guarda en un bloque auxiliar (sexto bloque), luego se reemplaza el bloque codificado $D \oplus E$ con el bloque auxiliar que contiene la información de D. Este proceso se repite hasta que la información del bloque A se obtiene y se valida con la firma S_{A}. Este proceso requiere un total de 96 bytes de RAM para almacenar los bloques que no han sido validados.

Para la validación de firmas, solo se recibe S_{D}. Después de decodificar el bloque A, se calcula la firma S_{A} con la firma del bloque anterior y A. Luego, con el código obtenido B y S_{A}, se calcula S_{B}. Este proceso se repite para calcular S_{C} y luego S_{D}, validando la cadena completa si S_{D} recibido coincide con el calculado. Este proceso requiere 48 bytes de RAM

para almacenar las firmas en uso.

Finalmente, la cantidad máxima de RAM requerida estará determinada por el algoritmo que tenga las mayores exigencias en términos de uso de memoria. El algoritmo de criptografía asimétrica nunca se ejecutará de forma simultánea con la recepción de bloques de datos. Por lo tanto, la RAM máxima necesaria será el valor mayor entre la RAM requerida por el cifrado asimétrico o la suma de la RAM requerida por el cifrado simétrico y la RAM necesaria para el peor escenario posible.

La simulación del peor escenario en una ESP32 resultó en un uso de 29,764 bytes de memoria flash y 424 bytes de RAM (combinando Ascon-128a con el peor caso). Posteriormente, la implementación completa de la propuesta requirió 95,552 bytes de memoria flash y un máximo de 800 bytes de RAM. En el caso del microcontrolador ATMEGA328P, los requerimientos fueron de 1,698 bytes de memoria flash y 214 bytes de RAM. Finalmente, la implementación completa en este microcontrolador necesitó 13,250 bytes de memoria flash y 545 bytes de RAM (cifrado asimétrico).

5.2.3. Seguridad de la Propuesta

En esta sección, se abordan diversos escenarios de ataque y se evalúa analíticamente la robustez de la propuesta en términos de seguridad bajo dichos escenarios.

Seguridad de Hardware

Primero, consideramos el problema de la seguridad de hardware. Nuestra propuesta demuestra una alta robustez contra las técnicas de criptoanálisis de hardware debido a que la implementación de la curva secp256r1 cuenta con contramedidas de software integradas en la librería micro-ecc. Además, Ascon-128a es altamente resistente a ataques de canal lateral, ya que no presenta fugas de información temporal y sus s-boxes están implementadas con operaciones lógicas bit a bit. Desde un punto de vista del criptoanálisis clásico, los cifrados utilizados no presentan vulnerabilidades conocidas y son ampliamente reconocidos y recomendados por la comunidad científica.

Ataques de Intercepción de Paquetes (Sniffing Attacks)

El siguiente escenario evaluado es la intercepción de paquetes, también conocido como sniffing attacks. Dado que utilizamos un canal inalámbrico, no podemos evitar la escucha de las transmisiones. Sin embargo, nuestro esquema de seguridad emplea encriptación de extremo a extremo, por lo que solo con escuchar el mensaje no se puede acceder a la información. Por tanto, nuestra propuesta es robusta contra este tipo de ataques.

Ataques de Suplantación de Identidad (Spoofing Attacks)

En cuanto a los ataques de suplantación de identidad (spoofing attacks), estos se vuelven ineficaces cuando se aplican a dispositivos protegidos con nuestra propuesta, ya que la autenticidad está sujeta a un intercambio seguro de llaves. Un atacante tendría que limitarse a retransmitir lo que un dispositivo o la estación base transmiten, sin poder entender

dicha información. Aunque este ataque puede ser dañino al mantener a un nodo aislado, la información se mantiene confidencial.

Escenarios donde se Busca Afectar la Infraestructura de Salud

La infraestructura de salud está protegida por cifrado robusto que puede ejecutarse en dispositivos de altas prestaciones, como AES-256, SHA-3 y firmas agregadas BLS [83, 84]. Desde el punto de vista criptográfico, esta infraestructura es sólida. Además, debido a la naturaleza distribuida de blockchain, los registros no pueden manipularse sin que se note ni acceder a ellos sin las credenciales indicadas. Finalmente, debido a que proponemos el uso de una blockchain de consorcio, es altamente improbable que hayan nodos mal intencionados dentro de la red.

Escenarios no Abordados

Finalmente, abordamos dos escenarios para los cuales nuestra propuesta no es suficiente. El primer tipo de ataque son los ataques de denegación de servicio y ataques de jamming. Para estos ataques, es necesario tomar medidas adicionales que se consideran en trabajos futuros. El segundo tipo de ataque no abordado en nuestra propuesta son los ataques de inyección de fallas por hardware. Cabe destacar que estos ataques pueden tener contramedidas, como la propuesta en [9], donde una parte de las placas que contienen a los microprocesadores es modificada para mitigar las fallas inyectadas.

Capítulo 6

Conclusiones

En esta tesis, se propone el uso de blockchain para el envío de información en arquitecturas LPWAN aplicadas a eHealth. Para abordar esta problemática, se llevó a cabo una exhaustiva revisión bibliográfica de algoritmos criptográficos, identificando la curva secp256r1 para el intercambio de claves y Ascon-128a para el cifrado simétrico como las opciones más adecuadas para estos dispositivos de recursos limitados. Ambos algoritmos ofrecen un nivel de seguridad de 128 bits, permitiendo implementar un mecanismo de autenticación que cumple con el nivel 2 de seguridad establecido por la norma IEEE 802.15.6. Este innovador encadenamiento de información en los esquemas de transmisión garantiza la confidencialidad, integridad, no repudio y autenticidad de los datos.

Además, la confiabilidad se incrementó mediante la introducción de esquemas de transmisión basados en codificación, lo que resultó en mejoras significativas en la cobertura de la transmisión. La cobertura se evaluó en el punto donde se alcanzaba una probabilidad de interrupción de 0.1. Los resultados mostraron que todos los esquemas de comunicación duplicaron aproximadamente su alcance en comparación con las transmisiones sin ningún tipo de redundancia. Específicamente, el mejor esquema codificado logró una cobertura de 16.1 km, mientras que el mejor esquema basado en réplicas idénticas alcanzó una cobertura de 14.2 km. Además, los esquemas codificados superaron a los de réplicas idénticas en todas las tasas de transmisión evaluadas. Estos esquemas se analizaron utilizando los parámetros de NB-IoT mientras que el largo de la firma y el bloque de información fueron derivados de los largos de las salidas de los algoritmos criptográficos. También se analizó el rendimiento de los esquemas bajo diferentes condiciones de red, estos fueron evaluados utilizando un modelo de desvanecimiento Nakagami-m, para tres valores de m, incluyendo Rayleigh como caso especial. Se observa que la tendencia de los esquemas se mantiene, aunque la relación entre ellos varía en función de la distancia. Por lo tanto, la decisión sobre qué esquema utilizar para cada dispositivo de recursos limitados también depende de las condiciones de línea de vista con respecto a la estación base.

Los algoritmos criptográficos identificados en la revisión bibliográfica fueron evaluados en microcontroladores populares, como el ESP32 WROOM-32D y el ATMEGA328P, permitiendo determinar cuáles son los más adecuados para estos dispositivos. Los resultados mostraron una ventaja significativa de Ascon-128a sobre AES-128 en la ESP32, donde Ascon-128a re-

quirió solo el 60 % del tiempo de cifrado y el 34 % del tiempo de descifrado comparado con AES-128, lo que implica un menor consumo energético. En cuanto al uso de memoria, Ascon-128a demostró ser más eficiente, utilizando solo un 11 % de la memoria flash y un 4,7 % de la RAM en comparación con AES-128. Por otro lado, al comparar los algoritmos de intercambio de llaves con cifrado asimétrico, no se observaron ventajas claras entre las curvas secp256r1 y Curve25519, sugiriendo que su elección dependerá del dispositivo de implementación. Finalmente, se simuló el peor escenario para un esquema codificado con el fin de estimar el uso máximo de memoria requerido por la propuesta completa. Los resultados indicaron que, en la ESP32, este esquema utilizaría apenas un 2,3 % de la memoria flash y un 0,2 % de la RAM. En el caso del ATMEGA328P, los requerimientos fueron del 5,2 % de la memoria flash y del 26,6 % de la RAM.

Por último, se realizó un análisis de los vectores de ataque mitigados por el esquema de seguridad propuesto y se abordaron las demás capas de la arquitectura LPWAN, proponiendo medidas de seguridad específicas para cada una. Los resultados demuestran que los esquemas codificados son superiores a los esquemas de repetición tradicionales y, al mismo tiempo, son lo suficientemente simples para su implementación en dispositivos de recursos limitados, ofreciendo una solución segura y fiable.

6.1. Trabajo Futuro

Como parte del trabajo futuro, se planea implementar el esquema de transmisión completo, incluyendo pruebas empíricas para evaluar la confiabilidad del enlace inalámbrico en escenarios reales. Además, se investigará la robustez de estos esquemas en entornos adversos, estudiando su comportamiento frente a ataques de interferencia, como el *jamming*, y el impacto de ataques coordinados desde múltiples nodos adversarios.

Se extenderá el análisis al enlace ascendente, donde se utilizará la SINR (Signal-to-Interference-plus-Noise Ratio) para evaluar la confiabilidad del canal, debido a que la interferencia es más significativa en este enlace, especialmente en escenarios con un alto número de dispositivos transmitiendo simultáneamente. Además, se llevará a cabo un análisis detallado de las colisiones que pueden ocurrir en el enlace ascendente, lo cual es crucial para evaluar la capacidad del sistema en situaciones de congestión.

Asimismo, se realizarán comparaciones empíricas de la efectividad del esquema propuesto frente a distintas tecnologías LPWAN, lo que permitirá evaluar su desempeño en términos de cobertura, consumo energético y resistencia a interferencias. Por otro lado, se llevarán a cabo pruebas de penetración para identificar posibles vulnerabilidades de *hardware* relacionadas con el esquema criptográfico y evaluar su efectividad en escenarios reales. Finalmente, se profundizará en el proceso de generación y búsqueda de información dentro de la base de datos distribuida, con el objetivo de validar su eficiencia y desempeño en situaciones prácticas.

Bibliografía

[1] Statista, "Internet of Things - Worldwide," 2024. Accessed: January 3, 2024.

[2] K. Zandberg, K. Schleiser, F. Acosta, H. Tschofenig, and E. Baccelli, "Secure firmware updates for constrained iot devices using open standards: A reality check," *IEEE access*, vol. 7, pp. 71907–71920, 2019.

[3] International Organization for Standardization, "Iso/iec 27001 and related standards information security management," 2022.

[4] J. Almalki, W. Al Shehri, R. Mehmood, K. Alsaif, S. M. Alshahrani, N. Jannah, and N. A. Khan, "Enabling blockchain with iomt devices for healthcare," *Information*, vol. 13, no. 10, p. 448, 2022.

[5] A. Yohan and N.-W. Lo, "An over-the-blockchain firmware update framework for IoT devices," in *2018 IEEE Conference on Dependable and Secure Computing (DSC)*, pp. 1–8, IEEE, 2018.

[6] M. Rana, Q. Mamun, and R. Islam, "Lightweight cryptography in IoT networks: A survey," *Future Generation Computer Systems*, vol. 129, pp. 77–89, 2022.

[7] V. A. Thakor, M. A. Razzaque, and M. R. A. Khandaker, "Lightweight Cryptography Algorithms for Resource-Constrained IoT Devices: A Review, Comparison and Research Opportunities," *IEEE Access*, vol. 9, pp. 28177–28193, 2021.

[8] N. Ruminot, C. Estévez, V. D. Pegorara Souto, R. D. Souza, and S. Montejo-Sánchez, "Improving the reliability of lightweight blockchain lpwan transmission schemes," *IEEE Sensors Journal*, pp. 1–1, 2024. Early Access.

[9] N. Ruminot, C. Estevez, and S. Montejo-Sánchez, "A Novel Approach of a Low-Cost Voltage Fault Injection Method for Resource-Constrained IoT Devices: Design and Analysis," *Sensors*, vol. 23, no. 16, p. 7180, 2023.

[10] A. Astrin, "Ieee standard for local and metropolitan area networks part 15.6: Wireless body area networks," *IEEE Std 802.15.6*, 2012.

[11] United States Congress, "Health insurance portability and accountability act of 1996 (hipaa)." `https://www.govinfo.gov/app/details/PLAW-104publ191`, 1996. Accessed: 2024-09-27.

[12] European Union, "General data protection regulation." https://gdpr-info.eu/, 2016. Accessed: 2024-09-27.

[13] República de Chile, "Ley nº 19.628 sobre proteccion de la vida privada." https://www.bcn.cl/leychile/navegar?idNorma=141599&idVersion=2023-05-09, 2023. Accessed: 2024-09-27.

[14] World Health Organization, "Global observatory for ehealth," 1948. Accessed: 2024-09-27.

[15] Oh, Hans and Rizo, Carlos and Enkin, Murray and Jadad, Alejandro and others, "What Is eHealth (3): A Systematic Review of Published Definitions," *Journal of medical Internet research*, vol. 7, no. 1, p. e110, 2005.

[16] M. U. Mahfuz, *Internet of Medical Things*, pp. 661–664. Cham: Springer International Publishing, 2020.

[17] T. D. Mou and G. Srivastava, *Network Protocols for the Internet of Health Things*, pp. 21–66. Cham: Springer International Publishing, 2022.

[18] S. A. Ajagbe, J. B. Awotunde, A. O. Adesina, P. Achimugu, and T. A. Kumar, *Internet of Medical Things (IoMT): Applications, Challenges, and Prospects in a Data-Driven Technolog*, pp. 299–319. Singapore: Springer Nature Singapore, 2022.

[19] R. Hireche, H. Mansouri, and A.-S. K. Pathan, "Security and Privacy Management in Internet of Medical Things (IoMT): A Synthesis," *Journal of Cybersecurity and Privacy*, vol. 2, no. 3, pp. 640–661, 2022.

[20] J.-P. A. Yaacoub, M. Noura, H. N. Noura, O. Salman, E. Yaacoub, R. Couturier, and A. Chehab, "Securing internet of medical things systems: Limitations, issues and recommendations," *Future Generation Computer Systems*, vol. 105, pp. 581–606, 2020.

[21] N. Li, M. Xu, Q. Li, J. Liu, S. Bao, Y. Li, J. Li, and H. Zheng, "A review of security issues and solutions for precision health in Internet-of-Medical-Things systems," *Security and Safety*, vol. 2, p. 2022010, 2023.

[22] A. Avinashiappan and B. Mayilsamy, *Internet of Medical Things: Security Threats, Security Challenges, and Potential Solutions*, pp. 1–16. Cham: Springer International Publishing, 2021.

[23] X.-T. Dang, R. Knauer, S. Peters, and F. Sivrikaya, "A converged cloud-fog architecture for future ehealth applications," in *2021 Sixth International Conference on Fog and Mobile Edge Computing (FMEC)*, pp. 1–8, IEEE, 2021.

[24] B. Farahani, M. Barzegari, F. S. Aliee, and K. A. Shaik, "Towards collaborative intelligent iot ehealth: From device to fog, and cloud," *Microprocessors and Microsystems*, vol. 72, p. 102938, 2020.

[25] P. Danzi, A. E. Kalor, C. Stefanovic, and P. Popovski, "Repeat-authenticate sche-

me for multicasting of blockchain information in IoT systems," *2019 IEEE Globecom Workshops*, 2019.

[26] D. Koutras, G. Stergiopoulos, T. Dasaklis, P. Kotzanikolaou, D. Glynos, and C. Douligeris, "Security in iomt communications: A survey," *Sensors*, vol. 20, no. 17, p. 4828, 2020.

[27] "IEEE Standard for Telecommunications and Information Exchange Between Systems - LAN/MAN - Specific Requirements - Part 15.1: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Wireless Personal Area Networks (WPANs)," 2002.

[28] "IEEE Standard for Information technology–Telecommunications and information exchange between systems Local and metropolitan area networks–Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications," 2020.

[29] "IEEE Standard for Low-Rate Wireless Networks," *IEEE Std 802.15.4-2020 (Revision of IEEE Std 802.15.4-2015)*, pp. 1–800, 2020.

[30] B. Kim, S. Kim, M. Lee, H. Chang, E. Park, and T. Han, "Application of an internet of medical things (iomt) to communications in a hospital environment," *Applied Sciences*, vol. 12, no. 23, p. 12042, 2022.

[31] M. Pérez, F. E. Sierra-Sánchez, F. Chaparro, D. M. Chaves, C.-I. Paez-Rueda, G. P. Galindo, and A. Fajardo, "Coverage and energy-efficiency experimental test performance for a comparative evaluation of unlicensed lpwan: Lorawan and sigfox," *IEEE Access*, vol. 10, pp. 97183–97196, 2022.

[32] M. Iqbal, A. Y. M. Abdullah, and F. Shabnam, "An application based comparative study of LPWAN technologies for IoT environment," in *2020 IEEE Region 10 Symposium (TENSYMP)*, pp. 1857–1860, IEEE, 2020.

[33] O. Liberg, M. Sundberg, E. Wang, J. Bergman, and J. Sachs, *Cellular Internet of Things: Technologies, Standards, and Performance*. Academic Press, 1st ed., 2017.

[34] LoRa Documentation, "LoRa Documentation," 2023. Accessed: 2023-06-26.

[35] M. Z. Khan, O. H. Alhazmi, M. A. Javed, H. Ghandorh, and K. S. Aloufi, "Reliable Internet of Things: Challenges and Future Trends," *Electronics*, vol. 10, no. 19, 2021.

[36] D. Zhang, S. Mumtaz, and K. Huq, "Chapter 2 - SISO to mmWave massive MIMO," in *mmWave Massive MIMO* (S. Mumtaz, J. Rodriguez, and L. Dai, eds.), pp. 19–38, Academic Press, 2017.

[37] Y. Sun, I. Kadota, R. Talak, and E. Modiano, *Age of information: A new metric for information freshness*. Springer Nature, 2022.

[38] Y. Lee, "Freshness ratio of information: a new metric for age of information," *Electronics*

Letters, vol. 56, no. 3, pp. 139–141, 2020.

[39] G. Caso, O. Alay, L. De Nardis, A. Brunstrom, M. Neri, and M.-G. Di Benedetto, "Empirical Models for NB-IoT Path Loss in an Urban Scenario," *IEEE Internet Things J.*, vol. 8, no. 17, pp. 13774–13788, 2021.

[40] Y. Mo, M.-T. Do, C. Goursaud, and J.-M. Gorce, "Optimization of the predefined number of replications in a Ultra Narrow Band based IoT network," in *Wireless Days (WD)*, pp. 1–6, 2016.

[41] J. M. d. S. Sant'Ana, S. Montejo-Sánchez, R. D. Souza, and H. Alves, "Non-Orthogonal Replication Scheme for ALOHA Uplink in LPWAN," *IEEE Trans Ind. Informat.*, pp. 1–10, 2023.

[42] R. Ma, L. Xing, and Y. Wang, "Performance analysis of Reed-Solomon codes for effective use in survivable wireless sensor networks," *International Journal of Mathematical, Engineering and Management Sciences*, vol. 5, no. 1, p. 13, 2020.

[43] M. K. Roberts and P. Anguraj, "A comparative review of recent advances in decoding algorithms for Low-Density Parity-Check (LDPC) codes and their applications," *Archives of Computational Methods in Engineering*, vol. 28, no. 4, pp. 2225–2251, 2021.

[44] J. Huang, Z. Fei, C. Cao, and M. Xiao, "Design and analysis of online fountain codes for intermediate performance," *IEEE Trans Commun*, vol. 68, no. 9, pp. 5313–5325, 2020.

[45] S. Montejo-Sanchez, C. A. Azurdia-Meza, R. D. Souza, E. M. G. Fernandez, I. Soto, and A. Hoeller, "Coded Redundant Message Transmission Schemes for Low-Power Wide Area IoT Applications," *IEEE Wireless Commun. Lett.*, vol. 8, no. 2, pp. 584–587, 2019.

[46] J. M. D. S. Sant'Ana, A. Hoeller, R. D. Souza, S. Montejo-Sanchez, H. Alves, and M. D. Noronha-Neto, "Hybrid Coded Replication in LoRa Networks," *IEEE Trans Ind. Informat.*, vol. 16, no. 8, pp. 5577–5585, 2020.

[47] A. Goldsmith, *Wireless Communications*. United States of America by Cambridge University Press, New York, 2005.

[48] G. B. Arfken, H. J. Weber, and F. E. Harris, *Mathematical methods for physicists: a comprehensive guide*. Academic press, 2011.

[49] T. Kitahara, R. Hira, Y. Hara-Azumi, D. Miyahara, Y. Li, and K. Sakiyama, "Optimized software implementations of ASCON, Grain-128AEAD, and TinyJambu on ARM Cortex-M0," in *2022 Tenth International Symposium on Computing and Networking Workshops (CANDARW)*, pp. 316–322, IEEE, 2022.

[50] O. Hyncica, P. Kucera, P. Honzik, and P. Fiedler, "Performance evaluation of symmetric cryptography in embedded systems," in *Proc. 6th IEEE Int. Conf. Intell. Data Acquis. Adv. Comput. Syst.*, pp. 277–282, 2011.

[51] C. Gewehr, N. Moura, L. Luza, E. Bernardon, N. Calazans, R. Garibotti, and F. G. Moraes, "Hardware Acceleration of Authenticated Encryption with Associated Data via RISC-V Instruction Set Extensions in Low Power Embedded Systems," in *2024 IEEE 15th Latin America Symposium on Circuits and Systems (LASCAS)*, pp. 1–5, IEEE, 2024.

[52] C. Haldankar and S. Kuwelkar, "Implementation of AES and blowfish algorithm," *International Journal of Research in Engineering and Technology*, vol. 3, no. 03, pp. 143–146, 2014.

[53] M. Panda, "Performance analysis of encryption algorithms for security," in *International Conference on Signal Processing, Communication, Power and Embedded System (SCOPES)*, pp. 278–284, 2016.

[54] S. Rizvi, S. Z. Hussain, and N. Wadhwa, "Performance analysis of AES and TwoFish encryption schemes," in *2011 International Conference on Communication Systems and Network Technologies*, pp. 76–79, IEEE, 2011.

[55] I. A. Landge and B. Mishra, "VHDL based Blowfish implementation for secured embedded system design," in *2017 Third International Conference on Advances in Electrical, Electronics, Information, Communication and Bio-Informatics (AEEICB)*, pp. 497–501, IEEE, 2017.

[56] N. B. Silva, D. F. Pigatto, P. S. Martins, and K. R. Branco, "Case studies of performance evaluation of cryptographic algorithms for an embedded system and a general purpose computer," *Journal of Network and Computer Applications*, vol. 60, pp. 130–143, 2016.

[57] W. Diehl, F. Farahmand, A. Abdulgadir, J.-P. Kaps, and K. Gaj, "Face-off between the CAESAR Lightweight Finalists: ACORN vs," tech. rep., Ascon," Cryptology ePrint Archive 2019/184, 2019.

[58] M. J. Dworkin, E. B. Barker, J. R. Nechvatal, J. Foti, L. E. Bassham, E. Roback, and J. F. Dray Jr, "Advanced encryption standard (aes)," 2001.

[59] M. S. Turan, K. A. McKay, Ç. Çalik, D. Chang, L. Bassham, *et al.*, "Status report on the first round of the NIST lightweight cryptography standardization process," *National Institute of Standards and Technology, Gaithersburg, MD, NIST Interagency/Internal Rep.(NISTIR)*, vol. 108, 2019.

[60] National Institute of Standards and Technology (NIST), "Lightweight Cryptography Timeline," 2022. Checked on 2024-07-02.

[61] C. Dobraunig, M. Eichlseder, F. Mendel, and M. Schläffer, "Ascon v1.2," *CAESAR Competition*, 2014.

[62] T. M. Chen, J. Blasco, and H. Kupwade Patil, *Cryptography in WSNs*, pp. 783–820. Springer International Publishing, 2019.

[63] C. Paar and J. Pelzl, *Understanding cryptography: a textbook for students and practi-*

tioners. Springer Science & Business Media, 2009.

[64] N. Gura, A. Patel, A. Wander, H. Eberle, and S. C. Shantz, "Comparing Elliptic Curve Cryptography and RSA on 8-bit CPUs," in *Cryptographic Hardware and Embedded Systems - CHES* (M. Joye and J.-J. Quisquater, eds.), (Berlin, Heidelberg), pp. 119–132, Springer Berlin Heidelberg, 2004.

[65] S. Wu and Y. Zhu, "A Resource Efficient Architecture for RSA and Elliptic Curve Cryptosystems," in *2006 International Conference on Communications, Circuits and Systems*, vol. 4, pp. 2356–2360, 2006.

[66] M. Savari, M. Montazerolzohour, and Y. E. Thiam, "Comparison of ECC and RSA algorithm in multipurpose smart card application," in *Proceedings Title: International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec)*, pp. 49–53, 2012.

[67] K. Maletsky, "RSA vs ECC comparison for embedded systems," tech. rep., Microchip Technology, 2015.

[68] M. Suárez-Albela, T. M. Fernández-Caramés, P. Fraga-Lamas, and L. Castedo, "A Practical Performance Comparison of ECC and RSA for Resource-Constrained IoT Devices," in *Global Internet of Things Summit (GIoTS)*, pp. 1–6, 2018.

[69] M. Adalier and A. Teknik, "Efficient and secure elliptic curve cryptography implementation of curve p-256," in *Workshop on elliptic curve cryptography standards*, vol. 66, pp. 2014–2017, 2015.

[70] T. Silde, "Comparative study of ECC libraries for embedded devices," *Norwegian University of Science and Technology, Tech. Rep*, 2019.

[71] M. A. Mehrabi and C. Doche, "Low-cost, low-power FPGA implementation of ED25519 and CURVE25519 point multiplication," *Information*, vol. 10, no. 9, p. 285, 2019.

[72] S. Ullah and R. Zahilah, "Curve25519 based lightweight end-to-end encryption in resource constrained autonomous 8-bit IoT devices," *Cybersecurity*, vol. 4, pp. 1–13, 2021.

[73] M. B. Niasar, R. El Khatib, R. Azarderakhsh, and M. Mozaffari-Kermani, "Fast, small, and area-time efficient architectures for key-exchange on Curve25519," in *2020 IEEE 27th Symposium on Computer Arithmetic (ARITH)*, pp. 72–79, IEEE, 2020.

[74] M. Düll, B. Haase, G. Hinterwälder, M. Hutter, C. Paar, A. H. Sánchez, and P. Schwabe, "High-speed Curve25519 on 8-bit, 16-bit, and 32-bit microcontrollers," *Designs, Codes and Cryptography*, vol. 77, no. 2, pp. 493–514, 2015.

[75] M. Bertaccini, *Cryptography Algorithms: A guide to algorithms in blockchain, quantum cryptography, zero-knowledge protocols, and homomorphic encryption*. Packt Publishing Ltd, 2022.

[76] W. Easttom, *Modern Cryptography: Applied Mathematics for Encryption and Informa-*

tion Security. Springer Cham, 2nd ed., 2022.

[77] N. I. of Standards and T. (NIST), "SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions," 2012. Accessed on: 2024-01-06.

[78] A. Zniti and N. E. Ouazzani, "Hash algorithm comparison through a PIC32 microcontroller," *Bulletin of Electrical Engineering and Informatics*, vol. 12, no. 4, pp. 2457–2463, 2023.

[79] S. Abed, R. Jaffal, B. J. Mohd, and M. Al-Shayeji, "An analysis and evaluation of lightweight hash functions for blockchain-based IoT devices," *Cluster Computing*, vol. 24, pp. 3065–3084, 2021.

[80] D. Boneh, C. Gentry, B. Lynn, and H. Shacham, "Aggregate and verifiably encrypted signatures from bilinear maps," in *Advances in Cryptology—EUROCRYPT: International Conference on the Theory and Applications of Cryptographic Techniques, Warsaw, Poland, May 4–8, Proceedings 22*, pp. 416–432, Springer, 2003.

[81] H. Shu, P. Qi, Y. Huang, F. Chen, D. Xie, and L. Sun, "An efficient certificateless aggregate signature scheme for blockchain-based medical cyber physical systems," *Sensors*, vol. 20, no. 5, p. 1521, 2020.

[82] T.-H. Kim, G. Kumar, R. Saha, M. Alazab, W. J. Buchanan, M. K. Rai, G. Geetha, and R. Thomas, "CASCF: Certificateless aggregated signcryption framework for internet-of-things infrastructure," *IEEE Access*, vol. 8, pp. 94748–94756, 2020.

[83] N. T. M. Quan, "Attacks and weaknesses of bls aggregate signatures," *Cryptology ePrint Archive*, 2021.

[84] J. Burdges, O. Ciobotaru, S. Lavasani, and A. Stewart, "Efficient aggregatable BLS signatures with chaum-pedersen proofs." Cryptology ePrint Archive, Paper 2022/1611, 2022. `https://eprint.iacr.org/2022/1611`.

[85] S. Nakamoto *et al.*, "Bitcoin," *A peer-to-peer electronic cash system*, vol. 21260, 2008.

[86] Statista, "Consumo de electricidad anual de Bitcoin," 2023. Último acceso: 20 de junio de 2024.

[87] S. Küfeoğlu and M. Özkuran, "Bitcoin mining: A global review of energy and power demand," *Energy Research & Social Science*, vol. 58, p. 101273, 2019.

[88] C. Dannen, *Introducing Ethereum and solidity*, vol. 1. Springer, 2017.

[89] Hyperledger Fabric, "Hyperledger fabric." `https://www.hyperledger.org/use/fabric`, 2024. Accessed: 2024-07-03.

[90] Corda, "Corda." `https://www.corda.net/`, 2024. Accessed: 2024-07-03.

[91] Quorum, "Quorum." `https://docs.goquorum.consensys.io/`, 2024. Accessed: 2024-

07-03.

[92] Corda R3, "Corda r3." `https://r3.com/products/corda/`, 2024. Accessed: 2024-07-03.

[93] D. Lazar, H. Chen, X. Wang, and N. Zeldovich, "Why does cryptographic software fail? A case study and open problems," in *Proceedings of 5th Asia-Pacific Workshop on Systems*, pp. 1–7, 2014.

[94] B. Schneier, *Applied cryptography: protocols, algorithms, and source code in C*. john wiley & sons, 2007.

[95] P. C. Kocher, "Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems," in *Advances in Cryptology—CRYPTO'96: 16th Annual International Cryptology Conference Santa Barbara, California, Proceedings 16*, pp. 104–113, Springer, 1996.

[96] M. Randolph and W. Diehl, "Power side-channel attack analysis: A review of 20 years of study for the layman," *Cryptography*, vol. 4, no. 2, p. 15, 2020.

[97] A. Gangolli, Q. H. Mahmoud, and A. Azim, "A Systematic Review of Fault Injection Attacks on IoT Systems," *Electronics*, vol. 11, no. 13, 2022.

[98] N. Ruminot-Ahumada, C. Valencia-Cordero, and R. Abarzúa-Ortiz, "Side Channel Attack Countermeasure for Low Power Devices with AES Encryption," in *IEEE International Conference on Automation/XXIV Congress of the Chilean Association of Automatic Control (ICA-ACCA)*, pp. 1–7, IEEE, 2021.

[99] M. Hell and O. Westman, "Electromagnetic side-channel attack on AES using low-end equipment," *ECTI Transactions on Computer and Information Technology (ECTI-CIT)*, vol. 14, no. 2, pp. 139–148, 2020.

[100] P. Yang, F. Luo, Q. Ou, and D. Zhou, "Design and analysis of clock fault injection for aes," in *International Conference on Computer Communication and Network Security (CCNS)*, pp. 87–91, IEEE, 2020.

[101] O. T. Ltci, L. S. Ltci, and J.-L. D. Ltci, "Characterization of electromagnetic fault injection on a 32-bit microcontroller instruction buffer," in *Asian Hardware Oriented Security and Trust Symposium (AsianHOST)*, pp. 1–6, IEEE, 2020.

[102] R. Banoth and R. Regar, "Modern cryptanalysis methods, advanced network attacks and cloud security," in *Classical and Modern Cryptography for Beginners*, pp. 167–215, Springer, 2023.

[103] R. Vishwakarma and A. K. Jain, "A survey of DDoS attacking techniques and defence mechanisms in the IoT network," *Telecommunication Systems*, vol. 73, no. 1, pp. 3–25, 2020.

[104] Y. Al-Hadhrami and F. K. Hussain, "DDoS attacks in IoT networks: a comprehensive

systematic literature review," *World Wide Web*, vol. 24, no. 3, pp. 971–1001, 2021.

[105] N. López-Vilos, C. Valencia-Cordero, C. Azurdia-Meza, S. Montejo-Sánchez, and S. B. Mafra, "Performance analysis of the ieee 802.15.4 protocol for smart environments under jamming attacks," *Sensors*, vol. 21, no. 12, 2021.

[106] H. Pirayesh and H. Zeng, "Jamming Attacks and Anti-Jamming Strategies in Wireless Networks: A Comprehensive Survey," *IEEE Communications Surveys Tutorials*, vol. 24, no. 2, pp. 767–809, 2022.

[107] C. E. Shannon, "A mathematical theory of communication," *Bell System Technical Journal*, vol. 27, no. 3, pp. 379–423, 1948.

[108] R. Ahmad and I. Alsmadi, "Machine learning approaches to iot security: A systematic literature review," *Internet of Things*, vol. 14, p. 100365, 2021.

[109] N. M. Kumar and P. K. Mallick, "The internet of things: Insights into the building blocks, component interactions, and architecture layers," *Procedia computer science*, vol. 132, pp. 109–117, 2018.

[110] F. Khan, A. A. Al-Atawi, A. Alomari, A. Alsirhani, M. M. Alshahrani, J. Khan, and Y. Lee, "Development of a model for spoofing attacks in internet of things," *Mathematics*, vol. 10, no. 19, 2022.

[111] S. A. Ansar, S. Arya, S. Aggrawal, S. Saxena, A. Kushwaha, and P. C. Pathak, "Security in iot layers: Emerging challenges with countermeasures," in *Computer Vision and Robotics: Proceedings of CVR 2022*, pp. 551–563, Springer, 2023.

[112] H. Aldabbas and R. Amin, "A novel mechanism to handle address spoofing attacks in sdn based iot," *Cluster Computing*, vol. 24, no. 4, pp. 3011–3026, 2021.

[113] M. Lauridsen, H. Nguyen, B. Vejlgaard, I. Z. Kovacs, P. Mogensen, and M. Sorensen, "Coverage Comparison of GPRS, NB-IoT, LoRa, and SigFox in a 7800 km^2 Area," in *IEEE 85th Vehicular Technology Conference (VTC Spring)*, pp. 1–5, 2017.

[114] G. A. Akpakwu, B. J. Silva, G. P. Hancke, and A. M. Abu-Mahfouz, "A Survey on 5G Networks for the Internet of Things: Communication Technologies and Challenges," *IEEE Access*, vol. 6, pp. 3619–3647, 2018.

[115] Nokia, "LTE-M: Optimizing LTE for the Internet of Things," 2015.

[116] M. N. Alenezi, H. Alabdulrazzaq, and N. Q. Mohammad, "Symmetric encryption algorithms: Review and evaluation study," *International Journal of Communication Networks and Information Security*, vol. 12, no. 2, pp. 256–272, 2020.

[117] R. Rivest, "RFC1321: The MD5 message-digest algorithm," 1992.

[118] J. H. Burrows, "Secure hash standard," *Federal information processing standards publication*, pp. 180–1, 1995.

[119] N. S. H. Standard, "Technical Report FIPS 180-2," *National Institute of Standards and Technology*, 2002. https://csrc.nist.gov/files/pubs/fips/180-2/final/docs/fips180-2.pdf.

[120] N. I. of Standards and T. (NIST), "Lightweight Cryptography," 2023. Accessed: January 3, 2024.

[121] BLAKE2 — fast secure hashing, "Blake2." https://www.blake2.net/, 2024. Accessed: 2024-07-03.

[122] D. E. Ruíz-Guirola, C. A. Rodríguez-López, S. Montejo-Sánchez, R. D. Souza, O. L. López, and H. Alves, "Energy-efficient wake-up signalling for machine-type devices based on traffic-aware long short-term memory prediction," *IEEE Internet Things J.*, vol. 9, no. 21, pp. 21620–21631, 2022.

[123] rweather, "Arduino Cryptography Library," January 3, 2024.

[124] D. Labor, "AVR Crypto Library," January 3, 2024.

[125] S. Ha, H. Seo, Y. Moon, D. Lee, and J. Jeong, "A Novel Solution for NB-IoT Cell Coverage Expansion," in *Global Internet of Things Summit (GIoTS)*, pp. 1–5, 2018.

[126] N. Poursafar, M. E. E. Alahi, and S. Mukhopadhyay, "Long-range wireless technologies for IoT applications: A review," in *Eleventh International Conference on Sensing Technology (ICST)*, pp. 1–6, 2017.

Anexo

Artículos de Revista

- **Nicolás Ruminot-Ahumada**, Claudio Estévez, Victoria Dala Pegorara Souto, Richard Demo Souza, and Samuel Montejo-Sánchez, 'Improving the Reliability of Lightweight Blockchain LPWAN Transmission Schemes,' *IEEE Sensors Journal, Early Access, 2024. doi: 10.1109/JSEN.2024.2999999.*

- **Nicolás Ruminot-Ahumada**, Claudio Estévez, and Samuel Montejo-Sánchez, 'A Novel Approach of a Low-Cost Voltage Fault Injection Method for Resource-Constrained IoT Devices: Design and Analysis,' *Sensors, vol. 23, no. 16, pp. 7180, 2023.*