Street Art & Urban Creativity | Vol. 11, No. 7, 2025 | ISSN 2183-9956
Street Art & Urban Creativity. Scientific Journal
https://doi.org/10.62161/sauc.v11.6007

MEJORA DE LA FIABILIDAD DE LORAWAN MEDIANTE LA CALIBRACIÓN DE LA PLANIFICACIÓN DE RF Y LA REDUNDANCIA

RESULTADOS DE CAMPO PARA EL SISTEMA DE ALARMA CONTRA INUNDACIONES DIN

JOHNNY J MAFRA JR [1], DIOGO CARNEIRO RIBEIRO BUENO MARTINS [2]
[1] FITEC, BRASIL
[2] CEMIG, BRASIL

PALABRAS CLAVE

LoRaWAN
Fiabilidad
Disponibilidad
Alarma de inundación
Estudio del emplazamiento
Sniffer
Simulación RF

RESUMEN

Brasil alcanzó un récord histórico de 118 presas en situación de emergencia en 2023, lo que justificó el desarrollo de un sistema de alarma. Dada la falta de fiabilidad de LoRaWAN, principalmente en lo que respecta a los mensajes de enlace descendente, este trabajo presenta una solución para llevar la disponibilidad a los niveles más altos. Las alarmas se entregaron al 100 % en 5 minutos y FUOTA transmitió un firmware dividido en miles de fragmentos de forma fiable. También se presenta un enfoque para calibrar la simulación de RF para que se ajuste mejor a las mediciones. Esto elevó la disponibilidad del 77 % al 91 %. Para SNR por encima de -10 dB, la disponibilidad es tan buena como el 95 %.

RECIBIDO: 01/09/2025
ACEPTADO: 28/09/2025

1. Introducción: antecedentes de fallos en presas y revisión de trabajos relacionados

En lo que respecta a la historia de los fallos de presas, podemos señalar dos hitos importantes: el fallo de la presa de Mariana, en noviembre de 2015, y el de Brumadinho, en enero de 2019. Estas dos tragedias, que causaron cientos de muertes y daños medioambientales extensos en las cuencas fluviales, han llevado desde entonces el tema de los fallos de presas a los titulares. No obstante, la Ley brasileña n.º 12.334 de 2010 establece la Política Nacional de Seguridad de Presas, que define la zona de autorrescate como el área situada aguas abajo de la presa en la que no hay tiempo suficiente para que las autoridades intervengan en caso de emergencia. En estas zonas, la responsabilidad de notificar y alertar a la población recae directamente en el promotor de la presa.

La revisión de la Política Nacional de Seguridad de Presas por la Ley Federal n.º 14.066/2020 exige: «la instalación de un sistema de sonido u otra solución tecnológica más eficaz en situaciones de alerta o emergencia». Tradicionalmente, las alarmas de emergencia en las presas se proporcionan mediante sirenas de alta potencia, pero su infraestructura exige características robustas, como una activación remota fiable, supervisión y baterías. Por lo tanto, cada estación de sirenas es costosa de implementar.

Posteriormente, la Resolución n.º 95/2022 de la Agencia Nacional de Minería (ANM) estableció que, en el caso de las presas con un daño potencial asociado alto o medio, el promotor debe implementar sistemas de activación automática de sirenas, junto con otros mecanismos de alerta eficaces en la zona de autorrescate. Estos sistemas deben instalarse en lugares seguros, preferiblemente fuera de la zona de inundación, y contar con salvaguardias que garanticen su correcto funcionamiento incluso en caso de fallo. Además, el Plan de Acción de Emergencia para Presas Mineras debe incluir medidas específicas para alertar y evacuar a la población que reside en la zona de autorrescate, asegurando que todos conozcan los procedimientos a seguir en caso de emergencia.

La Agencia Nacional de Agua y Saneamiento (ANA) lleva desde 2011 registrando y clasificando las presas del país. Las presas se clasifican según su uso, como energía hidroeléctrica, riego, protección contra inundaciones, recreación, abrevadero para animales, regulación del caudal, contención de residuos industriales, contención de residuos mineros, uso industrial y protección del medio ambiente. También se clasifican por categorías como riesgo, daños potenciales asociados y volumen del embalse. En 2023, había 25.943 presas registradas en el Sistema Nacional de Información sobre Seguridad de Presas. De ellas, 1.591 están clasificadas como de riesgo medio o alto, con un gran potencial de daños asociados en caso de rotura (ANA, 2024). Teniendo esto en cuenta, el número de emergencias relacionadas con presas en Brasil alcanzó un máximo histórico de 118 en 2024, lo que supone un aumento significativo en comparación con los 94 casos registrados el año anterior. Este aumento se explica en parte por la aplicación de nuevas resoluciones de la ANM, como la Resolución n.º 175/2024, que establece normas más estrictas para la seguridad de las presas de residuos (ANM, 2024).

Cemig, una importante empresa brasileña dedicada a la generación, transmisión, distribución y comercialización de energía, fue pionera en el desarrollo de planes de emergencia para roturas de presas en sus centrales hidroeléctricas, habiendo iniciado estudios sobre el tema ya en 2003. La empresa cuenta con procedimientos para la inspección de campo, la recopilación y el análisis de datos de instrumentación, la preparación y revisión de planes de seguridad de presas, así como para la planificación y supervisión de los servicios de mantenimiento, el análisis de resultados y la clasificación de sus estructuras civiles. Actualmente se dispone de planes de emergencia específicos para cada presa. Desde 2018, la empresa mantiene su política de fortalecer las relaciones con las partes interesadas externas centradas en situaciones de emergencia, concretamente con las Oficinas Municipales de Coordinación de Defensa Civil y Protección.

El caso de las presas hidroeléctricas es único, ya que también se utilizan para regular el caudal de los ríos. Dicho esto, esto plantea un efecto secundario potencialmente grave, ya que el control del nivel de la presa, aunque sea para garantizar su propia seguridad, puede acabar recreando el

proceso de inundaciones naturales durante la temporada de lluvias. Además, cada año, las lluvias excesivas que se producen en las regiones cercanas a una presa hidroeléctrica pueden hacer que la zona sea susceptible de sufrir una inundación. Es decir, ni siquiera es necesario que se produzca un evento catastrófico en la propia presa para que se constituya una emergencia, lo que exige la emisión de una alerta.

LoRa es una tecnología diseñada específicamente para la recopilación de datos de sensores. De este modo, la mayoría de los estudios están relacionados con el diseño y la optimización de sensores, como la solicitud de repetición automática de enlace ascendente propuesta por Choi (Choi et al., 2020). En cualquier caso, algunos estudios abarcan el ámbito de la gestión de desastres, desde la recopilación de datos de sensores hasta la transmisión de alertas. Son aún menos los estudios dedicados a la mejora de la fiabilidad de las comunicaciones por radiofrecuencia.

Zhang presenta el diseño y la evaluación de un sistema de respuesta a emergencias y alertas de seguridad pública en tiempo real basado en el IoT, diseñado para la detección, clasificación y difusión rápidas de alertas durante incidentes críticos (Zhang et al., 2025). Utiliza varios tipos de RF, como Wi-Fi, 5G y LoRa. LoRa es específicamente un recurso alternativo para entornos rurales o de baja conectividad, ya que se basa en MQTT seguro sobre TLS. Se implementó un sistema prototipo en un entorno controlado para simular situaciones de emergencia del mundo real. Las alertas se envían a dispositivos móviles, paneles de control y salas de control.

En situaciones de emergencia, es posible que el servicio de comunicaciones móviles no esté disponible. Para estos casos, Sciullo propuso un sistema que consiste en una aplicación móvil conectada a un transceptor LoRa a través de Bluetooth Low Energy (BLE) (Sciulo et al., 2020). A través de la aplicación, los usuarios pueden enviar solicitudes de emergencia que son retransmitidas por otros pares hasta llegar a un personal de rescate capaz de manejar la emergencia.

Para mejorar la fiabilidad de las comunicaciones por radiofrecuencia, el artículo de Sisinni presenta un enfoque interesante que replica los mensajes en la capa de enlace de datos utilizando diferentes duraciones de chirp. Este esquema de repetición es un protocolo propuesto llamado LoRa-REP. Aumenta la probabilidad de que al menos una copia del mensaje se reciba correctamente (Sisinni et al., 2022).

El estudio de Rayess basado en simulaciones introduce la repetición ciega en LoRaWAN: un paquete se retransmite un número fijo de veces independientemente de su buena recepción. Aprovechando las funcionalidades existentes de la capa de enlace de datos, compara este modo redundante con dos modos existentes, a saber, el modo sin acuse de recibo y el modo con acuse de recibo (Rayes et al., 2023).

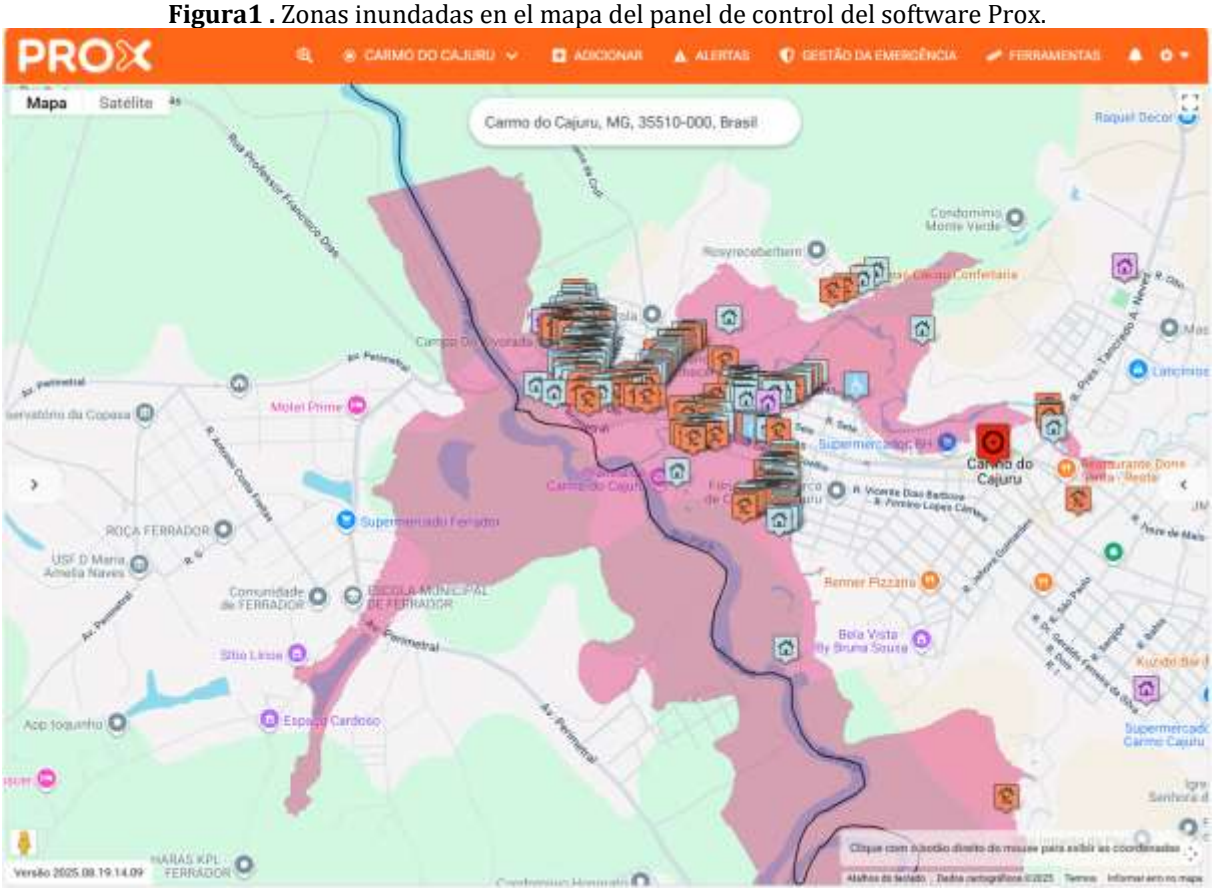
Un artículo de Coutaud sobre la optimización del algoritmo ADR (Adaptative Data Rate) presentó resultados experimentales sobre las tasas de entrega de paquetes en función de la SNR similares a los resultados obtenidos en este trabajo (Coutaud et al., 2020).

1.1. Solución de alarma de emergencia implementada

El sistema diseñado para proporcionar alarmas de emergencia se llama Prox. El proceso de su desarrollo consistió primero en el mapeo 3D de la zona de autorrescate y el valle del río aguas abajo, con el fin de determinar las áreas de inundación para cada tipo de evento, desde una lluvia ligera hasta una tormenta crítica, así como el desbordamiento y el colapso de la presa. El equipo de operaciones dispone de un panel de control con este mapeo, que se muestra enFigura1 . En su primer intento de implementar una alarma de emergencia, se optó por la vía tradicional, que consistía en instalar sirenas. Esto se hizo en 6 de las 32 centrales eléctricas de Cemig. Teniendo en cuenta su elevado coste y su eficacia limitada, el segundo paso fue incluir una alarma a través de una aplicación para teléfonos inteligentes, momento en el que se puso a disposición de todo el mundo una aplicación también llamada Prox a través de las tiendas de aplicaciones tradicionales. La aplicación lee la posición GPS de cada teléfono inteligente y, en caso de emergencia, siempre que la posición se encuentre dentro de la zona inundada, se envía una alarma a los dispositivos correspondientes. Al desarrollar la aplicación, se tuvo en cuenta la importancia de crear una

relación con los usuarios, con el objetivo de dar a conocer la importancia vital de estar al tanto de las alarmas.

Figura1 . Zonas inundadas en el mapa del panel de control del software Prox.



Fuente: Elaboración propia, 2025.

Dado que las presas y sus zonas de auto-rescate suelen estar situadas en zonas rurales remotas, lo más habitual es que no haya cobertura 4G, debido tanto a la distancia como a la topografía. De este modo, en 2020 se inició el desarrollo de una solución de cobertura para estas zonas. La tecnología elegida fue LoRaWAN debido a su largo alcance, bajo consumo energético y bajo coste. Debido a la alta potencia que necesitan las sirenas, es necesario utilizar varias bocinas, así como amplificadores de alta potencia, baterías grandes y sus respectivos controladores de carga de alta potencia. Todo ello se encuentra dentro de grandes cajas eléctricas instaladas en un poste robusto. Todo esto combinado supone un alto coste para la opción de las sirenas. Por su parte, el coste de la solución LoRaWAN es entre 5 y 10 veces menor, lo que supone una rentabilidad muy atractiva. Teniendo esto en cuenta, la solución descrita en este trabajo se ha instalado en 11 presas.

Para ello, se ha desarrollado un sistema LoRaWAN de extremo a extremo. El mismo software Prox gestiona el sistema, registra a los usuarios finales y envía las alarmas. La infraestructura LoRaWAN utiliza el servidor de red de código abierto Chirpstack, puertas de enlace LoRaWAN estándar, dispositivos finales denominados DIN (Dispositivos para Notificaciones Individuales) y una aplicación LoRaWAN denominada SND (Sistema para Notificaciones a DIN). La aplicación SND termina el protocolo de aplicación, gestionando las alarmas y administrando la red DIN. Esta solución se denomina Sistema DIN.

El dispositivo DIN ha sido cuidadosamente diseñado con el objetivo de armonizar con los hogares en los que estará presente (Horta & Damas, 2022) . Cuenta con una pantalla de tinta electrónica para mostrar mensajes, un zumbador para la alarma y una luz LED roja de alta intensidad que se ilumina en toda su cobertura para reforzar la alarma. Además, cuenta con una batería que lo mantiene en funcionamiento durante al menos 24 horas sin energía, algo que podría ocurrir en situaciones de emergencia, y un GPS para proporcionar su ubicación en tiempo real, al igual que los teléfonos inteligentes utilizados en el sistema Prox, lo que le permite enviar alarmas

únicamente a los dispositivos que se encuentran dentro de la zona inundada. Cuando funciona con normalidad, la pantalla muestra la fecha y la previsión meteorológica para el día actual y los tres días siguientes. Esto se hace para establecer una relación con los usuarios y ganarse su confianza, ya que demuestra que el sistema es fiable y garantiza a los usuarios que las emergencias recibirán una respuesta adecuada (Figura 2).

Sin embargo, cualquier sistema de comunicación es propenso a perder datos. Especialmente LoRaWAN, que está diseñado para redes con recursos limitados y optimizado para enviar mensajes de enlace ascendente (de Carvalho Silva et al., 2017). Esto significa que no hay garantía de que el mensaje llegue a su destino y que los mensajes de enlace descendente se pierdan más fácilmente, ya que no son la principal preocupación de LoRa. Se trata de una situación paradójica, ya que un sistema de alarma debe ser fiable. Por lo tanto, el objetivo de este artículo es mostrar la solución diseñada, implementada y validada para aumentar la fiabilidad de la comunicación LoRaWAN. Comprende la mejora de la cobertura de RF y la garantía de entrega de paquetes para alarmas y nuevas versiones de firmware.

Figura 2 . Dispositivo DIN que muestra la previsión meteorológica y la alarma.

Fuente: Elaboración propia, 2025.

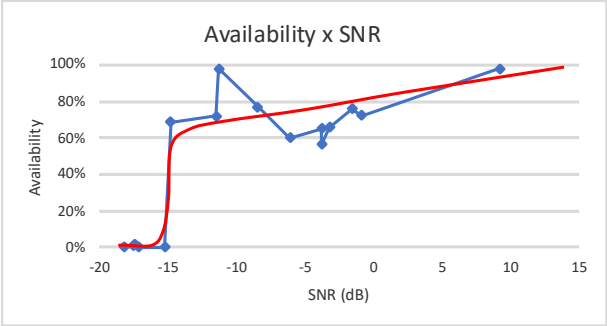
2. Método

2.1. Mejora de la cobertura de RF

LoRaWAN es muy sensible, por lo que tiene un gran alcance. Siendo así, con solo unas pocas puertas de enlace se podría cubrir una amplia zona. Sin embargo, incluso estando dentro de las especificaciones, la sensibilidad sigue estando limitada por la fiabilidad necesaria. En un trabajo anterior, se observó el comportamiento de la fiabilidad en relación con la calidad de la señal. La fiabilidad se representa mediante la disponibilidad de los paquetes de comunicación, que se mide por la relación entre los paquetes recibidos y los enviados. La calidad de la señal LoRaWAN se representa mediante su SNR. Se prefiere este indicador al RSSI porque se utiliza para controlar el SF (factor de dispersión) en el algoritmo ADR (velocidad de datos adaptativa). En Chirpstack, el servidor de red de código abierto utilizado, el parámetro principal que controla el ADR es el margen SNR. Calcula un margen SNR para cada enlace ascendente como el SNR máximo recibido a través de las pasarelas menos el SNR necesario para demodular la velocidad de datos actual (que depende del factor de dispersión). A continuación, toma el margen SNR máximo de un historial de enlaces ascendentes recientes (normalmente los últimos 20, aunque es configurable). Después de restar un margen de instalación configurado (por defecto 10 dB), el margen restante determina el número de pasos en los que se puede aumentar la velocidad de datos (cada paso es de aproximadamente 3 dB, lo que permite un cambio a una velocidad de datos más alta o a un factor de dispersión más bajo) y optimiza el índice de potencia de transmisión. Si el margen es insuficiente o se pierden los enlaces ascendentes (deducido de los contadores de tramas), se reduce la velocidad de datos para mejorar la fiabilidad (Chirpstack, 2025).Figura 3 (Leitão, et al., 2022) presenta la disponibilidad observada en una muestra de casi 20 dispositivos finales de los 40 desplegados en el campo, todos ellos con diferentes distancias, obstáculos de edificios y relieve. La disponibilidad es relativa a los enlaces ascendentes de un sistema AMI (Infraestructura de

Medición Avanzada), por lo tanto, difiere del caso de este artículo, que está asociado con el enlace descendente. Se puede observar que la disponibilidad aumenta de alrededor del 70 % a cerca del 100 % en función de la relación señal-ruido (SNR), excepto por debajo de -15 dB. Por debajo de este umbral, cae abruptamente a cerca de cero.

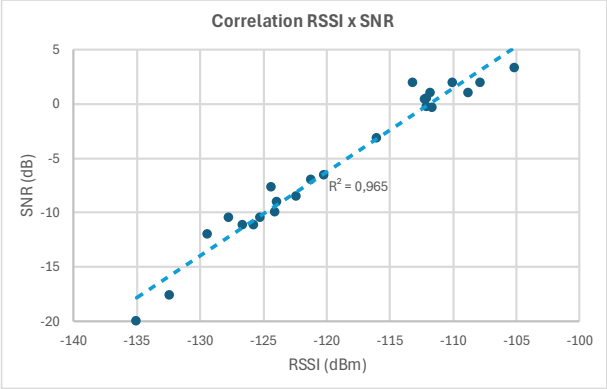
Figura 3 . Disponibilidad de LoRaWAN en función de la calidad de la señal.



Fuente: Leitão, et al., 2022.

Este comportamiento limitante se tuvo en cuenta en la estimación de RF. La SNR puede relacionarse linealmente con la RSSI, como se puede observar en los resultados obtenidos por las mediciones realizadas en este trabajo sobre el terreno, que se muestran enFigura4 . De esta manera, se seleccionó el límite de -120 dBm, que corresponde a una SNR entre -10 y -5 dB, dejando un margen de seguridad hasta el límite de -15 dB, y una disponibilidad cercana al 80 % segúnFigura 3 . El modelo de simulación se configuró implementando el modelo ITU-R P.1812.6, que se utiliza ampliamente en la evaluación detallada de los niveles de señal en los servicios terrestres de punto a área. Este modelo es aplicable a frecuencias entre 30 MHz y 6 GHz, cubre distancias de 250 m a 3000 km y tiene en cuenta el perfil del terreno en el cálculo de la propagación (UIT-R, 09/2021) . Para garantizar un margen de seguridad en la predicción de la cobertura, los parámetros de disponibilidad temporal y espacial se fijaron en el 95 %, lo que significa que el 95 % del tiempo (a lo largo del año) y en el 95 % de las ubicaciones, el nivel de señal estará por encima del valor previsto, lo que reduce la probabilidad de que se produzcan zonas de sombra o la indisponibilidad del servicio. El simulador se puede parametrizar fácilmente con este límite RSSI para generar los mapas de calor, lo que permite evaluar y optimizar la ubicación de las pasarelas.

Figura4 . Disponibilidad de LoRaWAN en función de la calidad de la señal.



Fuente: Elaboración propia, 2025.

2.2. Calibración de la simulación

Tras la primera implementación del sistema, quedó claro que existía una diferencia notable entre la simulación y las mediciones sobre el terreno, ya que los valores RSSI y SNR observados en el servidor de red eran diferentes de los calculados, ya que, lamentablemente, eran peores. Para contrarrestar esto, se desarrolló un proceso para calibrar la simulación. Consiste en una pasarela LoRaWAN móvil montada en un poste telescópico de 14 m de altura y un sniffer (Figura ***5***). El

sniffer es simplemente un dispositivo final LoRaWAN DIN con un firmware especial. Funciona de manera similar a un ping ICMP. Envía 10 solicitudes al software de aplicación y espera las respuestas. A continuación, presenta el número de respuestas, así como el valor mínimo, medio y máximo del RSSI y el SNR medidos. Funciona fijado en SF12 o DR0 para que los resultados sean comparables al eliminar esta variable. El DR de enlace descendente es una función de la velocidad de datos de enlace ascendente (LoRa Alliance, 2017). Dado que el enlace ascendente está fijado en DR0, se fijará en DR8 como la especificación AU915 utilizada en Brasil en el enlace descendente, es decir, siempre el más sensible en cada dirección.

Figura 5 . Poste de puerta de enlace móvil de 14 m y sniffer

Fuente: Elaboración propia, 2025.

Uno de los sitios (en los que se instaló el sistema) elegidos para llevar a cabo el procedimiento de calibración fue el que tenía la mayor cantidad de dispositivos finales, ya que proporcionaría un buen efecto estadístico. Por lo tanto, la siguiente debate se refiere a la región de Carmo do Cajuru, en el estado de Minas Gerais (Brasil), que cuenta con una presa de una central hidroeléctrica, operada por Cemig. Tras la primera fase de simulación y selección de los emplazamientos de las pasarelas, se realizaron estudios de campo en los emplazamientos. La pasarela móvil se colocó en cada uno de estos emplazamientos, mientras que el sniffer se llevó a varios puntos de interés para realizar mediciones de RSSI y SNR. De este modo se obtuvo el resultado que se muestra enFigura4
.

En la segunda ejecución de la simulación se modificaron los parámetros para garantizar que la predicción se ajustara a las condiciones ambientales reales. Se realizaron ajustes de forma iterativa, perfeccionando el modelo hasta que los valores obtenidos se situaron dentro de un margen de precisión aceptable en relación con las mediciones de campo. De esta forma, se ajustó el margen de desvanecimiento mediante el cambio de uno de sus componentes, el margen de confianza. La pérdida del cable y del conector también se ajustó a un valor más alto, a fin de incluir, además de sus propias pérdidas, el efecto de que el dispositivo final se encuentra en interiores en condiciones normales de uso. Una vez validado el modelo, se llevó a cabo un nuevo estudio simulando un conjunto actualizado de puntos de instalación.

2.3. Garantizar la entrega de la alarma

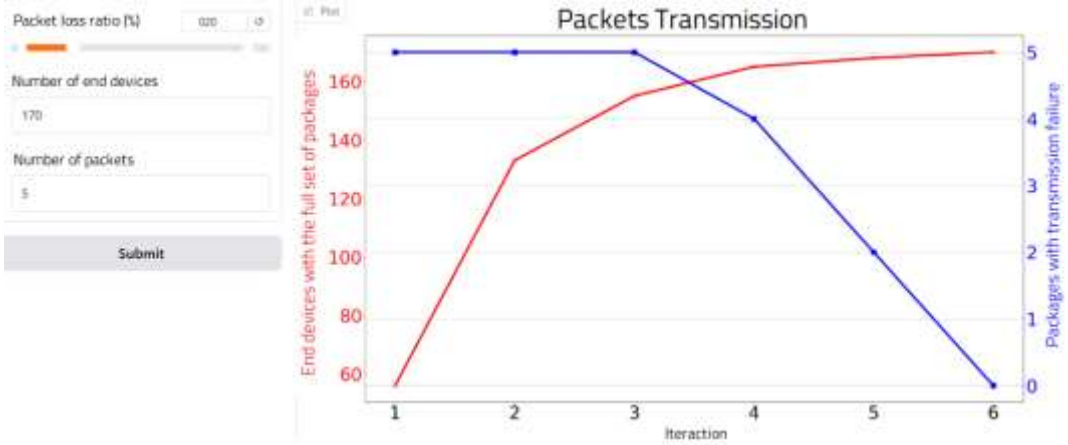
La mejora de la cobertura proporcionó buenos resultados, pero aún puede haber pérdida de paquetes. E incluso si se realizaran más mejoras, aún podría ocurrir. Esto hace que sea obligatorio

que un sistema de alarma proporcione medios para garantizar la entrega. Este requisito llevó al desarrollo del esquema de redundancia descrito en este trabajo.

Una alarma en el sistema DIN consiste en un paquete multicast descargado de la aplicación SND que contiene la alarma y la lista compactada de los dispositivos finales dentro del área de inundación, además de hasta cuatro paquetes que contienen el mensaje de texto que se va a mostrar. Esto se debe a que la pantalla permite mensajes de hasta casi 200 bytes, y el peor caso de paquete LoRaWAN es de alrededor de 50 bytes. De esta manera, habría un máximo de cinco paquetes. Como se ha comentado anteriormente, la simulación de RF se realizó teniendo en cuenta un límite en la relación señal-ruido (SNR) que proporciona una disponibilidad de alrededor del 80 % en el peor de los casos. Esto significa que se podría perder hasta un 20 % de los paquetes.

A continuación, se calculó el número de retransmisiones necesarias para garantizar una probabilidad del 100 % de recibir todos los paquetes, teniendo en cuenta que cada vez que se realiza una transmisión existe una probabilidad de pérdida del 20 %. La cifra obtenida fue de 6 retransmisiones. Para comprobar si esto funcionaría antes de su implementación sobre el terreno, se implementó un simulador que arrojó los resultados deFigura 6 .

Figura 6 . Simulación de retransmisión de paquetes teniendo en cuenta la tasa de pérdida.



Fuente: Elaboración propia, 2025.

Para mejorar aún más la fiabilidad de la alarma, una vez que un dispositivo final recibe una, envía un mensaje ACK de enlace ascendente. Dado que se compone de un solo paquete, las repeticiones calculadas fueron 5. Esto también se confirmó en el simulador presentado anteriormente.

Para verificarlo, se comprobó la probabilidad de pérdida del paquete ACK de enlace ascendente del dispositivo final debido a una colisión. El ACK tiene una longitud aproximada de 10 bytes y, en DR0, con una velocidad de transmisión de 250 bps, generará un paquete de 313 ms, que redondeamos a 500 ms para utilizarlo en el simulador de colisiones, otra herramienta desarrollada en este trabajo. Esta simulación mostró una probabilidad de colisión inferior al 20 %, que es nuestra referencia, para transmisiones ACK en 60 s en una población de 100 dispositivos finales en un sistema LoRaWAN de 8 canales.

En el lado de la aplicación SND, la duración del paquete de alarma a la velocidad de transmisión de bajada más lenta, DR8, es de 980 bps para transmitir 53 bytes, lo que supone 474 ms, que redondearemos a 0,5 s. Esto concuerda con la medición de 0,493 s obtenida. En otras palabras, la transmisión de 5 paquetes tarda al menos 2,5 s. Supondremos que son 5 s, ya que hay un retraso desconocido entre cada transmisión. Se implementó para enviar el doble de lo calculado, enviando 12 veces los 5 paquetes con un intervalo de 50 s entre cada uno, lo que tardó 10 minutos en completar la tarea.

El algoritmo implementado en el lado del dispositivo final considera que, desde el momento en que el dispositivo final recibe el primer paquete de alarma, debe comenzar a transmitir ACK con solicitud de confirmación, aleatorizados en 60 s e ignorando cualquier alarma similar recibida en los siguientes 50 segundos. Esto se repetirá 5 veces, hasta un período de tiempo de 5 minutos, y puede interrumpirse al recibir la primera confirmación.

Para detener la alarma, se debe repetir este mismo proceso para un comando de parada de alarma.

De esta manera, tras 6 transmisiones de alarma en 300 s, se garantiza que todos los DIN hayan recibido la alarma, tal y como se muestra en el cálculo y la simulación anteriores. El requisito es que este intervalo de tiempo sea inferior a 5 minutos en la zona de autorrescate, debido al tiempo estimado que tarda en llegar una ola provocada por la rotura de la presa. La transmisión ACK solo sirve para aumentar aún más la fiabilidad del sistema. Además, el software de gestión del sistema DIN, SND, tiene la información exacta de cada DIN que no ha recibido la alarma. Dado que pueden estar en juego vidas humanas, el operador puede tomar una decisión sobre la acción de contingencia en este caso, que podría ser incluso enviar un equipo de rescate.

2.4. FUOTA

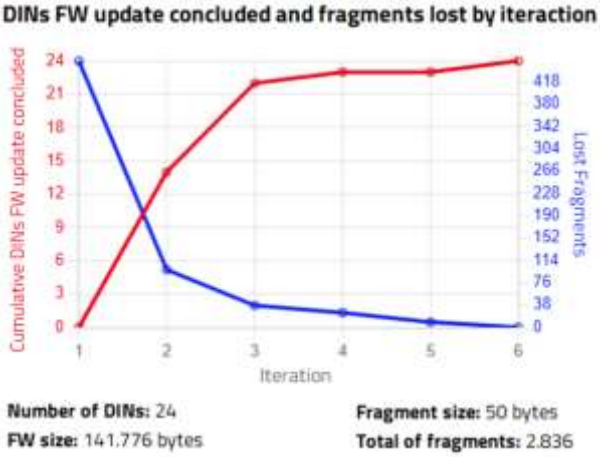
Teniendo en cuenta que el dispositivo final DIN tiene un firmware algo complejo, es propenso a sufrir errores. Para mantener la confianza en la solución, es obligatorio disponer de la posibilidad de actualizar el firmware de forma remota sin necesidad de retiradas. Incluso es necesario cumplir con nuevas normativas, como la CRA (Ley de Ciberresiliencia de la Unión Europea), que exigen la posibilidad de aplicar parches cuando se encuentra una vulnerabilidad (El Parlamento Europeo y el Consejo de la Unión Europea, 2024). La situación se complica aún más debido a que el firmware es considerablemente grande, del orden de cerca de 200 kB. Dado que, en el peor de los casos, los tamaños de los paquetes LoRaWAN son tan pequeños como 50 bytes, se necesitarían alrededor de 3.000 paquetes para transportar todo el firmware. Como se ha mencionado anteriormente, el parámetro considerado en este trabajo, que ha dimensionado el procedimiento de alarma, dio lugar a una tasa de pérdida de paquetes del 20 %. Pero podría haber DIN individuales con tasas peores que esa. Teniendo esto en cuenta, el esquema de actualización del firmware debe ser capaz de manejar todos estos requisitos tan exigentes.

La elección fue llevar al límite el esquema de redundancia presentado anteriormente. A pesar de que LoRaWAN tiene una especificación FUOTA (Firmware Update Over The Air), debe configurarse estimando la pérdida de paquetes. Además, como se indica en la especificación, no está diseñado para bloques de datos muy pequeños ni muy grandes debido a las limitaciones de la capa de enlace (limitación del ciclo de trabajo y tiempo de emisión prolongado) (LoRa Alliance, 2022) . Dado que la tasa de pérdida de paquetes puede variar según los distintos sitios e incluso según los DIN individuales, no es aplicable utilizar una tasa en el peor de los casos que se adapte a todos. Sería demasiado grande para varios sitios, lo que haría que el tiempo dedicado a la actualización del firmware fuera innecesariamente largo para muchos de ellos o demasiado corto para los críticos. El algoritmo desarrollado se basó en uno utilizado en trabajos anteriores sobre Wi-SUN, que tenía una solución probada y se implementó en miles de unidades en el campo (Mafra et al., 2015).

El algoritmo implementado para FUOTA envía la apertura del proceso con información como la identificación de la versión, el número de paquetes y el hash para verificar la integridad del firmware al final del proceso. A continuación, realiza la primera transmisión de cada uno de los miles de paquetes. Este primer paso puede llevar días, teniendo en cuenta el intervalo necesario entre cada uno para evitar colisiones. Una vez finalizado, SND envía una solicitud de paquetes faltantes. Para garantizar su recepción, el enlace descendente se envía 20 veces en intervalos de 30 segundos, lo que suma un total de 10 minutos. A continuación, cada DIN responde con los paquetes faltantes, que están limitados a 25 por vez, ya que el límite de tamaño de cada paquete es de alrededor de 50 bytes. Esto se realiza enviando enlaces ascendentes confirmados hasta 5 veces, ya que se trata de un solo paquete. A continuación, SND organiza todos los paquetes perdidos, eliminando las repeticiones y retransmitiéndolos. Este proceso se repite tantas veces como sea necesario, informando de hasta 25 paquetes perdidos, hasta que el último DIN recibe todos los paquetes. Al final, se verifica la integridad del firmware y se inicia su ejecución. Una ventaja de este proceso sobre el especificado por LoRaWAN es que solo necesita el tamaño del firmware para la memoria adicional, en lugar de su tamaño más la tasa de pérdida de paquetes estimada.

Figura 7 presenta la evolución de FUOTA para un índice medio de pérdida de paquetes de casi el 2 % obtenido en un entorno de laboratorio, contemplando 24 DIN y un firmware que se va a actualizar dividido en 2.836 paquetes. Los primeros pasos pueden comprender la totalidad de los paquetes, lo que lleva bastante tiempo. Después, se produce una disminución del número de paquetes, lo que también reduce el tiempo, haciendo que el proceso se acelere aún más en cada pasada. Solo se necesitaron 6 iteraciones y 28 horas para completar la actualización. Esto se debe a que el 2 % es un índice de pérdida de paquetes muy bajo y, al haber solo 24 dispositivos finales, se pudo establecer un intervalo de 30 segundos entre la transmisión de cada paquete sin degradación por colisión. De todos modos, si se produjera una colisión que causara la pérdida de paquetes, el algoritmo la repararía automáticamente.

Figura 7 . Evolución de FUOTA para un 2 % de pérdida de paquetes en un entorno de laboratorio.



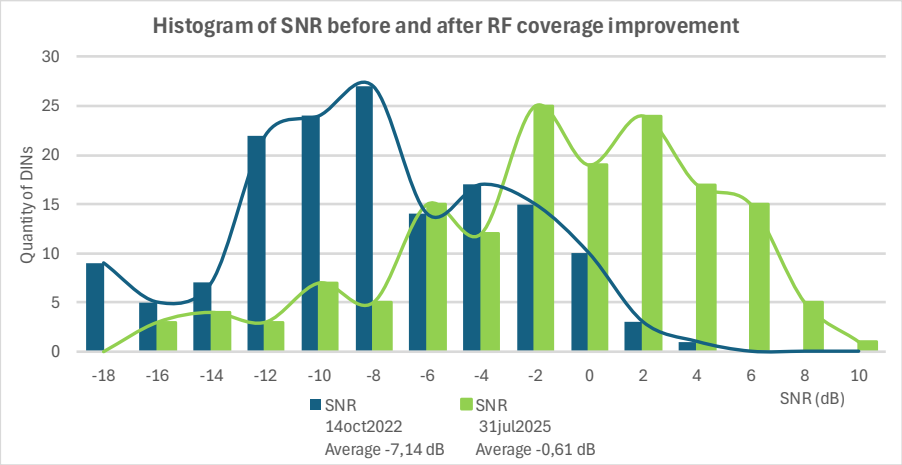
Fuente: Elaboración propia, 2025.

3. Resultados

3.1. Resultados de campo de la mejora de la cobertura

Como se ha indicado anteriormente, en el primer intento, la simulación de RF tuvo en cuenta el límite de -15 dB para la relación señal-ruido (SNR) que se encontró en el trabajo anterior y se instalaron dos pasarelas en la región. Sin embargo, los resultados no fueron tan buenos como se esperaba. De hecho, se estableció la comunicación, pero no con la disponibilidad necesaria para un sistema de alarma. Tras la calibración y la nueva simulación, se instalaron tres nuevas pasarelas. Figura 8 presenta el histograma de la SNR antes y después de su instalación para los aproximadamente 180 dispositivos finales distribuidos en la región. Quedó claro que, antes de que se observara razonablemente bien el límite de -15 dB, solo había unos pocos dispositivos finales por debajo del límite. Por lo tanto, el límite se desplazó de -15 dB a alrededor de -10 dB y la media pasó de -7,14 dB a -0,61 dB.

Figura 8 . Histograma de la relación señal-ruido (SNR) antes y después de la mejora de la cobertura de RF.

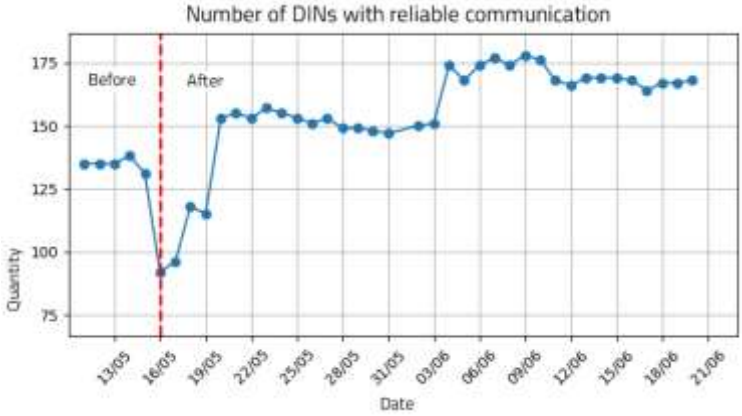


Fuente: Elaboración propia, 2025.

La disponibilidad se calculó utilizando los datos proporcionados por el software SND que gestiona los dispositivos finales. Se controla el número de paquetes transmitidos por SND que llegan realmente a los dispositivos finales. Para ello, SND cuenta y registra cuántos paquetes se enviaron cada día. Por otro lado, los dispositivos finales mantienen un registro acumulativo de cuántos paquetes han recibido y envían esta cifra en el paquete de latido horario. Gracias a ello, es posible calcular la disponibilidad diaria de cada dispositivo final, con una media mensual o una media por ubicación.

El número de dispositivos finales con comunicación fiable se mantuvo estable en torno a 130 antes de la instalación de las tres nuevas pasarelas, que comenzó el 16 de mayo. Durante el proceso, disminuyó ligeramente debido al cambio en la configuración necesaria en la red. Cuando la última pasarela nueva entró en funcionamiento el 4 de junio, el sistema alcanzó una nueva condición estable, con aproximadamente 170 DIN en línea (Figura 9). También se calculó que la disponibilidad media de esta ubicación antes de la instalación de las pasarelas era de alrededor del 77 % y que, después, mejoró hasta el 91 %.

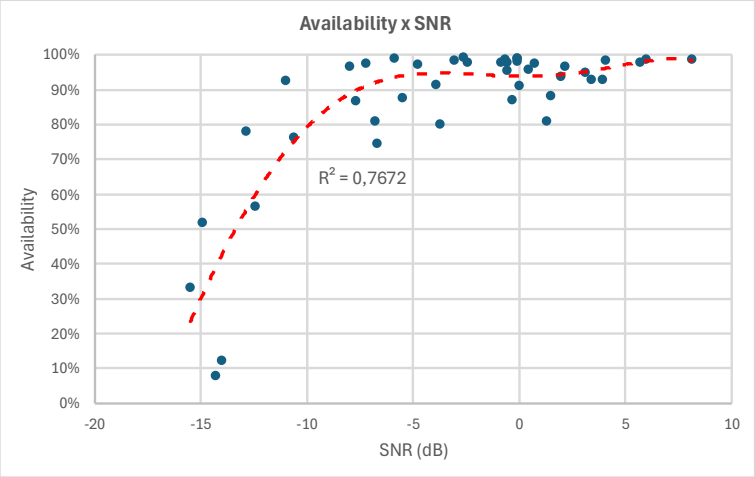
Figura 9 . Número de DIN con comunicación fiable.



Fuente: Elaboración propia, 2025.

También se calculó la disponibilidad de cada dispositivo final, teniendo en cuenta todos los periodos, tanto antes como después de la instalación de las nuevas pasarelas, para obtener datos con valores SNR débiles y fuertes. De este modo, se obtuvo el resultado que se presenta enFigura 10.

Figura 10 . Disponibilidad observada tras la mejora de la cobertura.

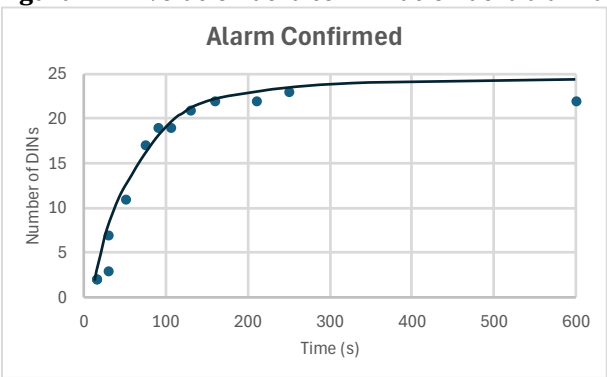


Fuente: Elaboración propia, 2025.

3.2. Resultados de campo de la alarma

La ubicación de la prueba de campo de la alarma es la misma que la validación de la calibración de la simulación de RF, Carmo do Cajuru. Como se ha indicado anteriormente, su disponibilidad media con las nuevas pasarelas instaladas se sitúa en torno al 91 %, es decir, una pérdida de paquetes del 9 %. En estas condiciones, se envió una alarma a 23 dispositivos finales seleccionados. Esto ilustra la función que permite enviar alarmas solo a los usuarios afectados por inundaciones, por ejemplo. Figura 11 muestra la evolución temporal de la recepción de la confirmación de la alarma yFuente: Elaboración propia, 2025.
Figura *12* presenta la captura de pantalla de la confirmación de la alarma por parte de todos ellos antes de 5 minutos.

Figura 11 . Evolución de la confirmación de la alarma.



Fuente: Elaboración propia, 2025.

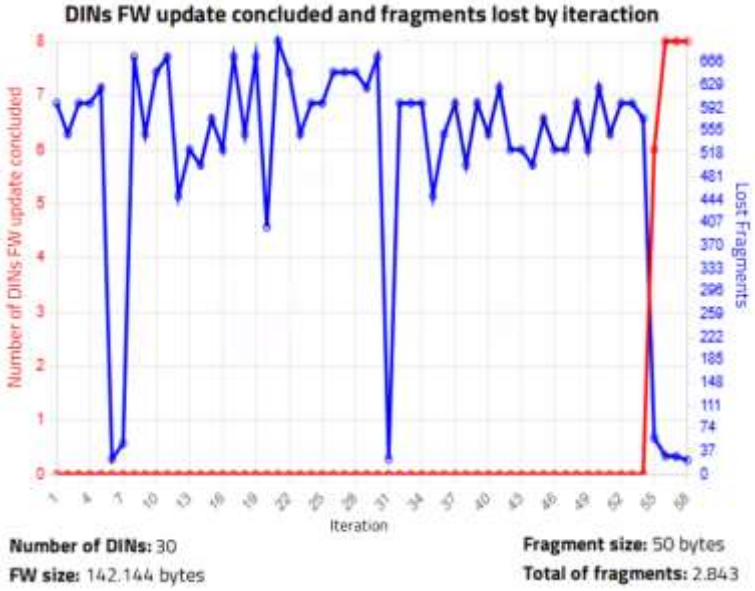
Figura 12 . Prueba satisfactoria de la alarma sobre el terreno.

Fuente: Elaboración propia, 2025.

3.3. Resultados de campo para FUOTA

La prueba de campo de FUOTA se realizó en la misma ubicación que las pruebas de campo anteriores; sin embargo, con el fin de forzar los límites, se llevó a cabo antes de la instalación de las nuevas pasarelas, cuando la disponibilidad media era de alrededor del 77 %, es decir, la tasa de pérdida de paquetes era del orden del 23 %, ligeramente por encima del límite teórico utilizado en nuestro dimensionamiento del sistema. Para la prueba se utilizaron 30 de los dispositivos finales. El resultado se presenta enFigura 13 .

Figura 13 . Evolución de FUOTA para un 23 % de pérdida de paquetes en el campo.



Fuente: Elaboración propia, 2025.

El proceso FUOTA también cuenta los paquetes perdidos. Por lo tanto, se calculó para esos 30 dispositivos finales específicos una tasa media de pérdida de paquetes del 18 %. Esto difiere ligeramente de la media del 23 % en la ubicación, incluyendo todos sus dispositivos finales.

4. Discusión

EnFigura 8 se observó que la calibración ajustó la intensidad de la señal en los puntos críticos y, por ello, la señal mejoró en general en los demás puntos, lo que provocó un aumento de la media de la relación señal-ruido en la región donde se instalaron las nuevas pasarelas. Esto también condujo a un aumento de la disponibilidad del 77 % al 91 %, lo que concuerda con el 95 % configurado en la simulación y valida el proceso de calibración.

El resultado presentado enFigura 10 , es coherente con el trabajo anterior, deFigura 3 y la bibliografía (Coutaud, Heusse, & Tourancheau, 2020) . En la Figura 10 los puntos de datos parecen ser más uniformes que en laFigura 3 porque la medición se tomó durante un período más largo, 35 días en lugar de 15, y con una muestra más grande, 48 muestras en lugar de 16. De todos modos, el resultado es el mismo: por encima de -15 dB de SNR, la disponibilidad mejora de manera muy sensible. EnFigura 10 es ligeramente superior porque está relacionado con el enlace descendente en lugar del ascendente, que tiene una menor sensibilidad en LoRa. Debido al menor ruido en la medición, es posible observar enFigura 10 que por encima de un valor de SNR entre -10 y -5 dB, la disponibilidad media (línea roja) es aproximadamente igual al 95 %, tal y como se parametrizó en el simulador de RF. Esto se debe sin duda a la calibración del proceso. Además, por encima de -10 dB, prácticamente todos los puntos de datos presentan una disponibilidad superior al 80 %. Este es un parámetro importante para medir la fiabilidad de los protocolos.

Figura 11 muestra que en menos de 180 s, o 3 minutos, el 95 % de los DIN han confirmado la alarma. En 5 minutos se confirman todos, como se muestra en la captura de pantalla deFuente: Elaboración propia, 2025.

Figura *12* . Es posible que la alarma haya llegado a los dispositivos finales mucho antes. Este es el tiempo que tarda en llegar la confirmación. Dado que el ACK se envía en ventanas de 60 s, repitiéndose hasta 5 veces para garantizar la entrega, esto explica por qué observamos esta duración en las pruebas.

Figura 13 muestra que se necesitaron un total de 60 iteraciones para completar el proceso FUOTA. Este número inesperadamente elevado de iteraciones se debió no solo al alto índice de pérdida de paquetes, sino también a la cantidad limitada de paquetes en la lista de paquetes perdidos del dispositivo final, solo 25. El dispositivo final podría necesitar hasta 600 fragmentos, como se muestra en la figura, pero solo puede solicitar 25 a la vez. Aun así, el proceso se completó después de casi 70 horas. Solo en la cuarta y última iteración, 6 dispositivos finales completaron el firmware, y los 8 restantes lo completaron en cada una de las tres últimas, lo que suma un total de 30 dispositivos.

5. Conclusión

La principal conclusión de este trabajo es que cualquier canal o tecnología de comunicación es propenso a la pérdida de paquetes, y que la solución para ello es la redundancia. Esto se demostró aquí mediante simulaciones, así como pruebas tanto en laboratorio como sobre el terreno para pequeñas cantidades de paquetes, como en el caso de la alarma, y para cantidades masivas de ellos, como en el caso de FUOTA. Si el sistema es lo suficientemente lento como para permitir el tiempo empleado, entonces se puede utilizar la redundancia. Este es el caso del sistema de emergencia presentado en este trabajo. En caso de inundación, normalmente se tarda un par de horas en enviar la alarma antes de que se abran las compuertas. En caso de colapso de la presa, el requisito es que se avise a la población hasta 5 minutos después de la activación de la alarma. Debido a todas las vidas en peligro, la fiabilidad es primordial y el operador debe tener una confirmación fiable de que se ha realizado con éxito.

La solución presentada en este trabajo puede utilizarse en cualquier tipo de canal de comunicación. Por ejemplo, ahora que NB IoT está disponible comercialmente, se ha añadido a DIN y las soluciones de alarma y FUOTA se han replicado con resultados similares. La ventaja es que los paquetes son más grandes, pudiendo alcanzar el tamaño estándar de Ethernet de 1500 bytes. NB IoT es una opción conveniente porque elimina la necesidad de instalar puertas de enlace. Sin embargo, en un país con un área tan extensa como Brasil, la región de las presas suele estar en zonas remotas y montañosas, por lo que normalmente no tiene cobertura comercial.

Los siguientes pasos consisten en finalizar la validación de la opción NB IoT para DIN, desarrollar un sniffer NB IoT que permita realizar estudios de campo para verificar la calidad de la señal en los sitios candidatos y mejorar algunas características. Un ejemplo de ello sería mejorar la convergencia de FUOTA, que se vio afectada negativamente por el límite de 25 paquetes en la lista de faltantes al utilizar LoRaWAN.

7. Agradecimientos

Nos gustaría dar las gracias a André dos Santos por las pruebas del sistema y el análisis de fallos, a Camila Alcamim por el diseño de RF y el despliegue sobre el terreno de las pasarelas LoRaWAN, a Eugênio Daher por la gestión del proyecto, a Evandro Aguiar por el desarrollo del firmware, a Fernando Silvestrow por el desarrollo de la aplicación SND, a Geraldo Caldas por el diseño del hardware, el suministro de muestras y la realización de pruebas de hardware, y a Samuel da Silva por las pruebas del sistema y el apoyo sobre el terreno. También agradecemos a Aneel, que financió este trabajo a través de su programa RDI.

Referencias

Agência Nacional de Águas e Saneamento Básico. (2024). *Relatório de segurança de barragens 2023*. https://www.snisb.gov.br/portal-snisb/api/file/download/714/4/rsb_2023_2024_06_27_11_01_28.pdf

Agência Nacional de Mineração. (2024, septiembre). *Report mensal – Barragens de mineração*. https://www.gov.br/anm/pt-br/assuntos/barragens/boletim-de-barragens-de-mineracao/boletim-mensal-setembro-2024.pdf/view

ChirpStack. (2025). *Adaptive data-rate (ADR)*. https://www.chirpstack.io/docs/chirpstack/features/adaptive-data-rate.html

Choi, R., Lee, S., & Lee, S. (2020). Reliability improvement of LoRa with ARQ and relay node. *Symmetry, 12*(4), 552. https://doi.org/10.3390/sym12040552

Coutaud, U., Heusse, M., & Tourancheau, B. (2020). High reliability in LoRaWAN. In *2020 IEEE 31st Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*. IEEE. https://doi.org/10.1109/PIMRC48278.2020.9217220

Horta, A., & Damas, P. (2022). Design, tecnologia e segurança: Impactos da morfologia de um dispositivo individual de notificação sobre a percepção de usuários em zonas de risco de rompimento de barragens. *Revista Design & Tecnologia, 12*(24), 113-133. https://doi.org/10.23972/det2022iss24pp01-10

International Telecommunication Union. (2021). *Recommendation ITU-R P.1812-6: A path-specific propagation prediction method for point-to-area terrestrial services in the frequency range 30 MHz to 6 000 MHz*. https://www.itu.int/dms_pubrec/itu-r/rec/p/R-REC-P.1812-6-202109-S!!PDF-E.pdf

Karthikeyan, R., Duraiarasu, E., Ganesh, K., & Bhagyalakshmi, L. (2024). LoRa and IoT based device for disaster and fleet management. *International Research Journal on Advanced Science Hub, 6*(5), 88–96. https://doi.org/10.47392/IRJASH.2024.016

Leitão, C. M., Strobel, F. de, Almeida, G. de, Mafra Júnior, J. J., Oliveira, J. J., & Xavier, R. C. (2022). *Solução AMI para áreas rurais dispersas e áreas urbanas com dificuldades de recepção de sinais utilizando tecnologia LoRa* [Conferência]. SENDI 2022 – Seminário Nacional de Distribuição de Energia Elétrica.

LoRa Alliance. (2017). *LoRaWAN™ regional parameters 1.1*. https://lora-alliance.org/wp-content/uploads/2020/11/lorawan-regional-parameters-v1.1ra.pdf

LoRa Alliance. (2022). *LoRaWAN fragmented data block transport specification TS004-2.0.0*. https://resources.lora-alliance.org/technical-specifications/ts004-2-0-0-fragmented-data-block-transport

Mafra, J. J., Jr., Hosami, M., Freitas, L., Martinelli, M., & Almeida, A. (2015). Hybrid communication module – Motivations, requirements, challenges and implementations. In *IEEE PES Innovative Smart Grid Technologies Latin America (ISGT LA)* (pp. 25–29). IEEE. https://doi.org/10.1109/ISGT-LA.2015.7381124

Rayess, J., Khawam, K., Lahoud, S., Helou, M. E., & Martin, S. (2023). Study of LoRaWAN networks reliability. In *2023 6th Conference on Cloud and Internet of Things (CIoT)* (pp. 200–205). IEEE. https://doi.org/10.1109/CIoT57267.2023.10084880

Sciullo, L., Trotta, A., & Di Felice, M. (2020). Design and performance evaluation of a LoRa-based mobile emergency management system (LOCATE). *Ad Hoc Networks, 96*, 101993. https://doi.org/10.1016/j.adhoc.2019.101993

Silva, J. de C., Rodrigues, J. J. P. C., Alberti, A. M., Šolić, P., & Aquino, A. L. L. (2017). *LoRaWAN – A low power WAN protocol for Internet of Things: A review and opportunities* [Conferência]. 2nd International Multidisciplinary Conference on Computer and Energy Science (SpliTech), Split, Croatia.

Sisinni, E., Carvalho, D. F., Ferrari, P., Flammini, A., & Gidlund, M. (2022). Adding redundancy to LoRaWAN for emergency communications at the factory floor. *IEEE Transactions on Industrial Informatics, 18*(10), 7332–7340. https://doi.org/10.1109/TII.2021.3124054

The European Parliament and the Council of the European Union. (2024). Regulation (EU) 2024/2847 of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) No 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act). *Official Journal of the European Union, L series*. http://data.europa.eu/eli/reg/2024/2847/oj

Zhang, H., Zhang, R., & Sun, J. (2025). Developing real-time IoT-based public safety alert and emergency response systems. *Scientific Reports, 15*, 13465. https://doi.org/10.1038/s41598-025-13465-7