

## RESUMEN

Desde hace unos años las Redes Inalámbricas de Sensores (WSN por sus siglas en inglés) han demostrado ser fundamentales en la implementación de paradigmas como el denominado Internet de las Cosas (IoT por sus siglas en inglés) o las ciudades inteligentes (*Smart Cities*). Sin embargo, por su forma de funcionamiento y entornos donde operan, este tipo de redes son susceptibles a errores o problemas durante su operación, debido principalmente a la influencia de factores de entorno. Además, al tratarse de sistemas distribuidos donde múltiples nodos (en algunos casos heterogéneos) colaboran en las tareas de sensorización, procesado de información y transmisión de los datos obtenidos; resulta extremadamente complejo evaluar su funcionamiento. La monitorización de las WSN, tanto durante su desarrollo, como en el despliegue o a lo largo de su vida útil, es la mejor forma con la que se puede observar cómo trabajan, ya sea con fines de depuración, verificación de su correcta instalación, o control de su operación.

Los monitores o plataformas de monitorización suelen clasificarse según su enfoque, bien *activo* o bien *pasivo*. Los monitores activos requieren algún nivel de modificación en el sistema monitorizado y permiten adquirir información más precisa de la operación de la WSN, pero pueden interferir con su funcionamiento. Por otro lado, los monitores pasivos no requieren modificación del sistema observado por lo que prácticamente no causan interferencia o intrusión en la misma, pero la información obtenida puede no ser suficiente. Existen también los bancos de pruebas (*testbeds*), que pueden funcionar tanto de forma pasiva (solo recolectando información de los nodos) como de forma activa (cuando también envían órdenes a estos), pero su uso está limitado a entornos de laboratorio.

Tradicionalmente, un monitor puede clasificarse como *hardware* o *software* en función de su naturaleza. También se ha definido un enfoque híbrido, donde se combinan elementos hardware y elementos software en el proceso de monitorización. En los últimos tiempos se ha denominado como híbrido a cualquier propuesta que combine al menos dos enfoques de funcionamiento. En este sentido, existen contadas propuestas híbridas de monitorización para WSN, pero están enfocadas a un tipo específico de nodos, su funcionamiento es limitado (solo pueden recoger cierta información), y en ocasiones solo se han presentado como propuesta teórica, sin alcanzar la fase de implementación que proporcione un monitor operativo.

En esta tesis se presenta la propuesta de una Plataforma de Monitorización Híbrida, denominada HMP (*Hybrid Monitoring Platform*), orientada a la evaluación del comportamiento de cualquier WSN. Esta plataforma busca combinar los enfoques de monitorización *activo* y *pasivo* para aprovechar las ventajas de ambos al tiempo que se compensan sus inconvenientes. La arquitectura de la plataforma sigue un Modelo de Referencia genérico para plataformas de monitorización distribuida. Este modelo busca que los sistemas o plataformas propuestos puedan ser aplicables a cualquier sistema distribuido, y específicamente a cualquier WSN, y que la

independencia de niveles permita compartimentar la problemática de cada nivel, y por tanto los avances en un nivel del modelo no impliquen cambios en los otros niveles. Esta independencia permitiría, además, simplificar la interoperabilidad entre plataformas.

En la plataforma propuesta pueden encontrarse tres tipos de componentes principales: Los Nodos Monitores, que se conectan de forma activa a los nodos de la WSN; los Nodos Espías (*Sniffer* en inglés), que capturan en el medio compartido los mensajes enviados por la aplicación WSN a monitorizar; y finalmente un Servidor de Monitorización. Los dos primeros componentes registran los eventos observados de la aplicación WSN a monitorizar, a la par que registran el instante de tiempo en que éstos ocurren, y los hacen llegar al tercero, encargado de coordinar la recolección de los datos obtenidos por los otros componentes, y su procesado. El Servidor de Monitorización procesa los datos obtenidos, combinándolos en una única traza que refleja el comportamiento global de la aplicación. Esta traza puede ser analizada para evaluar las prestaciones, optimizar el funcionamiento o detectar problemas durante el diseño, despliegue, sintonización u operación de la aplicación basada en WSN.

Todo ello es posible gracias a múltiples avances alcanzados en distintos aspectos de la plataforma de monitorización. Uno de ellos es la definición de la arquitectura genérica que permite la interoperabilidad, reutilización, y modularidad en el desarrollo de los elementos. Otro es la reducción de la intrusión causada por la operación de monitorización sobre los nodos de la WSN, especialmente desde el punto de vista de las transmisiones al Nodo Monitor. Otra de ellas es el novedoso mecanismo de sincronización de las marcas de tiempo de los datos obtenidos. Este mecanismo, denominado GTSO (*Global Trace Synchronization and Ordering Mechanism*), realiza una sincronización fuera de línea (es decir después de haber terminado la monitorización). Su funcionamiento es simple pero efectivo, como se demuestra en las pruebas realizadas. Además, evita que existan cambios en el orden correcto de los eventos registrados.

La plataforma completa ha demostrado su utilidad mediante la monitorización de una WSN real, obteniendo resultados satisfactorios, tales como la obtención de una traza completa y ordenada de los eventos de la red que refleja el comportamiento del sistema, así como la detección de funcionamientos incorrectos en la misma en base al análisis de la traza obtenida. Como valor añadido, gracias al enfoque basado en una arquitectura estructurada en niveles independientes, HMP puede ser aplicada de forma modular y sencilla a diversos tipos de WSN.