

Communication Network Model that supports a Sensing System based on Robustness Criteria

R. Córdova Estrella, I. Marin-Garcia, *Member IEEE*, A. Munoz-Arcenales, Victor Asanza, *Member IEEE*, and W. Velásquez, *Member IEEE*

Abstract—Proactive routing protocols are commonly used in wireless sensor networks due to their main feature is distributing information very quickly. However, most of the implementations using these protocols do not guarantee the robustness that unexpected emergencies required. In this paper, it tries to model a wireless sensor network implemented in a three-floor's building, robust enough to assure the working of the net despite of the loss of nodes in emergency situations. The performance of DSDV (Destination Sequenced Distance Vector) and OLSR (On Link State Routing) is simulated in various scenarios using a different number of nodes in the building. The results show that the OLSR protocol can achieve a better performance in terms of robustness in the proposed scenarios.

Keywords— DSDV, OLSR, MPRs, NS3, sensor node, sump, addressing, robustness criteria.

I. INTRODUCCIÓN

Los recientes avances en temas de micro-electrónica, comunicación inalámbrica y dispositivos digitales ha permitido la evolución de las redes de sensores inalámbricas, que son ampliamente usadas en aplicaciones médicas, militares, de seguridad, entre otras. A pesar del crecimiento de este tipo de redes, existen algunos factores como latencia, redundancia y robustez que no son considerados durante el diseño de una red, lo que limita el rendimiento [1].

Los sistemas de redes de sensores son implementados sin considerar los ambientes hostiles y condiciones adversas a las que estos dispositivos podrían estar expuestos, tales como: incendios, altas temperaturas, cambios en los niveles de humedad, generación de humo y desastres naturales. Estos eventos podrían ocasionar la colisión de estructuras y con ello caída de enlaces o pérdida de paquetes, que afectan al desempeño normal de la red [2][3].

R. Córdova Estrella was with Escuela Superior Politécnica del Litoral, ESPOL, Campus Gustavo Galindo, Km 30.5 Vía Perimetral, P.O. Box 09-01-5863, Guayaquil, Ecuador, e-mail: robancor@espol.edu.ec

I. Marin-Garcia is with Escuela Superior Politécnica del Litoral, ESPOL, Campus Gustavo Galindo, Km 30.5 Vía Perimetral, P.O. Box 09-01-5863, Guayaquil, Ecuador, e-mail: imaringa@espol.edu.ec

A. Munoz-Arcenales was with Escuela Superior Politécnica del Litoral, ESPOL, Campus Gustavo Galindo, Km 30.5 Vía Perimetral, P.O. Box 09-01-5863, Guayaquil, Ecuador, e-mail: joanmuno@espol.edu.ec

Victor Asanza is with Escuela Superior Politécnica del Litoral, ESPOL, Campus Gustavo Galindo, Km 30.5 Vía Perimetral, P.O. Box 09-01-5863, Guayaquil, Ecuador, e-mail: vasanza@espol.edu.ec

W. Velásquez was with Escuela Superior Politécnica del Litoral, ESPOL, Campus Gustavo Galindo, Km 30.5 Vía Perimetral, P.O. Box 09-01-5863, Guayaquil, Ecuador, e-mail: wavelasq@espol.edu.ec

El modelo propuesto en este trabajo consiste en una red de comunicaciones que soporta un sistema de sensores basado en criterios de robustez. Esta red ha sido diseñada para un edificio de tres pisos de las siguientes dimensiones: (21 m, 16 m, 3 m) largo, ancho y alto respectivamente, donde los nodos de sensores son numerados y distribuidos en cada planta del edificio, con la finalidad de que puedan detectar y alertar oportunamente ante alguna situación de fallo. Para realizar la simulación se utiliza el software NS3.23 [4] que permite implementar dos protocolos de enrutamiento proactivo DSDV [5] y OLSR [6], uno orientado a elegir la siguiente ruta a partir de un número de secuencia y el otro un conjunto de vecinos MPRs (Multi-Point Relay) para establecer rutas óptimas.

El presente artículo está dividido en cinco secciones. La sección II presenta el estado del arte con las tecnologías a analizar. La sección III indica las condiciones de la simulación, configuración, caso de estudio y distribución de los nodos en el edificio. La sección IV se muestran las pruebas y resultados obtenidos en la simulación, Finalmente se presentan las conclusiones del estudio.

II. ESTADO DEL ARTE

Las Redes de Sensores Inalámbricas (WSN) están consideradas como plataformas de computación versátiles para varias aplicaciones de monitoreo y control. Estas redes son por lo general implementadas y luego dejadas desatendidas en ambientes que pueden sufrir de condiciones adversas, puesto que operan en ambientes hostiles se utilizan técnicas eficientes para proveerse de una plataforma de comunicación, procesamiento robusto y tolerancia a fallas. El alto consumo de energía debido a los sensores y demás componentes de la red, afectan en gran manera la calidad de vigilancia y monitoreo de la red de sensores; por ello se necesita tomar en cuenta lo siguiente [9] [10]:

- **Red Ad-Hoc**- Red de nodos que no necesita de un Punto de Acceso o red cableada para poder transmitir datos entre sí, con la tecnología inalámbrica 802.11; tienen la capacidad de compartir información con sus nodos adyacentes generando caminos de enrutamiento, logrando la comunicación entre todos, para el caso del sistema de sensores todos los nodos convergen en un nodo sumidero, el cual posee las tablas de enrutamiento y estado de conexión de todos [6], [7].
- **Grado nodal promedio (k)**- Es la característica de conectividad más común de cualquier topología, se le llama así al número de conexiones que tiene un nodo. Las redes que tengan un k más alto están en promedio

“mejor conectadas”, por consecuencia, es probable que sean más robustas; lo que significaría que existen más posibilidades de establecer conexiones [8].

- **Conectividad de los nodos**- Esta métrica representa el número más pequeño de nodos cuya remoción resulta en un grafo desconectado o de un solo nodo. La conectividad puede también ser definida como el número más pequeño de caminos entre dos nodos [8].
- **Heterogeneidad**- Es la desviación estándar del grado nodal promedio dividido por el grado nodal promedio. Mientras menor sea la magnitud de la heterogeneidad, mayor será la robustez de la topología [8]
- **Longitud de camino más corto**- Es calculada como el promedio de todos los caminos más cortos entre todos los posibles pares de nodos origen-destino de la red. Las redes con número de longitud de camino más corto son más robustas porque en respuesta a cualquier tipo de problema, es probable que pierdan un menor número de conexiones [8].
- **Radio de simetría**- El radio es esencialmente el cociente entre el número de distintos eigen-valores (resultados obtenidos de la matriz de adyacencia de la red) y del diámetro de la red. Por lo tanto, en redes de alta simetría, con valores de simetría entre 1 y 3, el impacto de perder un nodo no depende de qué nodo exactamente se pierda, lo que significa que la red funciona de manera equitativa en respuesta a un ataque aleatorio (SR) o a un ataque intencionado (ST). Las redes aleatorias por lo general, no tienen altos valores de simetría. Sin embargo, para grafos aleatorios, donde los nodos tienen la misma importancia en sentido estadístico puesto que los enlaces se ubican aleatoriamente, ningún nodo está privilegiado en el diseño. Esta condición no puede aplicarse en redes de mundo pequeño o en redes libres de escala [8], [10].
- **Latencia**- Suma de retardos temporales de una red producidos por la demora en la propagación y transmisión de datos a la hora de envío o recibido de paquetes; el tamaño de la información a enviar junto con la capacidad de almacenamiento de los buffers, son puntos claves para determinar una alta o baja latencia.
- **Conectividad de vecinos**- Esta métrica provee información sobre los vecinos que se encuentren a una distancia de 1 salto alrededor de un nodo, es calculada como el grado de vecinos promedio del grado de nodos promedio k.

La Robustez de la red y equipos de comunicación es necesaria en sistemas de sensores, debido a las condiciones adversas que se pueden alterar el funcionamiento normal de las aplicaciones. En este estudio son evaluados los protocolos de enrutamiento proactivos:

- **DSDV**- Es un protocolo de enrutamiento típico que está basado en el algoritmo Bellman-Ford distribuido. Cada ruta tiene una etiqueta con un número de secuencia, el cual es creado por el destino que indica el tiempo desde que la ruta fue realizada; los nodos manejan su propio

número de secuencia asignando un nuevo número dos veces más grande que el anterior. Cuando se recibe una actualización de ruta con un número de secuencia más alto, se reemplaza la ruta anterior, en caso de que existan rutas diferentes con el mismo número de secuencia, la ruta con la mejor métrica es elegida [5]. Un ejemplo básico de cómo opera el protocolo DSDV es mostrado en la Fig. 1 en donde se muestra la tabla de enrutamiento con los campos necesarios para hacer el enrutamiento centrado en el nodo 4 junto con el gráfico de la topología de red que se usó para generar dicha tabla.

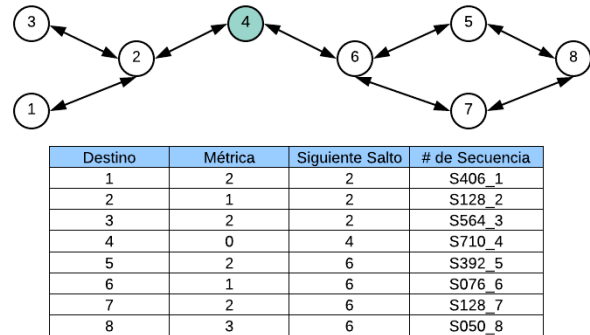


Tabla de enrutamiento del Nodo 4

Fig. 1 Tabla y modelo de enrutamiento en la red.

- **OLSR**- Es un protocolo de enrutamiento que usa el esquema de estado de enlace de forma optimizada para difundir información topológica a través de la red, su operación consiste principalmente en actualizar y mantener la información en unas tablas; cuyos datos están basados en el tráfico de control recibido. Su principal objetivo es minimizar el tráfico de control seleccionando un pequeño número de nodos conocidos como MPR (Multi Point Relays); los cuales establecen rutas óptimas hacia el destino de la red, este protocolo es adecuado para redes grandes [6]. En la Fig. 2 se muestra como ejemplo, una topología básica basada en el protocolo OLSR, en donde se muestran los nodos designados como MPR y como es el proceso de inundación y descubrimiento de la red.

A pesar de los protocolos de enrutamientos reactivos presentan un mejor desempeño en escenarios de emergencias, no son considerados en este estudio, sino más bien, serán utilizados para realizar una comparación a futuro en esta investigación.

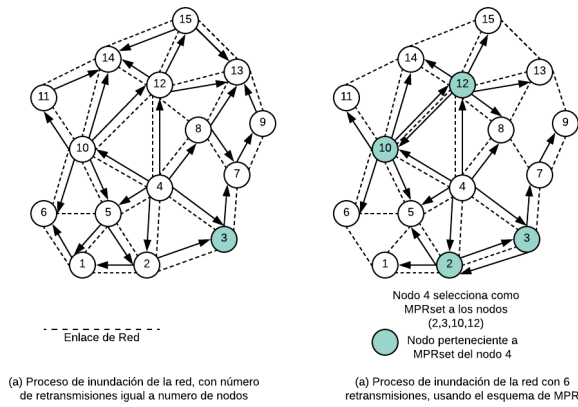


Fig. 2 Proceso de Inundación y descubrimiento de la red en OLSR.

III. CONDICIONES DE LA SIMULACIÓN

Para diseñar e implementar una red de comunicaciones es primordial conocer el funcionamiento de los protocolos, estándares y los canales inalámbricos que son usados para comunicaciones entre nodos. Adicionalmente, existen otros factores que se deben considerar como la protección física y la limitación en términos de energía que poseen los dispositivos. Estas restricciones hacen que las redes de sensores inalámbricas sean vulnerables a la falla de nodos o destrucción física de los mismos, el agotamiento de energía y el atasco de los canales inalámbricos provocados por mal rendimiento del protocolo utilizado. Los escenarios previamente descritos son simulados en NS3, con el fin de evaluar el desempeño de la red cuando es sometida a diferentes protocolos de enrutamiento proactivos: DSDV y OLSR [11] [12].

La Fig. 3 presenta la distribución en porcentaje de nodos sensores para cada piso, la misma que ha sido realizada en base a la cantidad de nodos que van a ser simulados. Así, la planta baja cuenta con el 40% de los nodos considerados en esta investigación, siendo éste el piso con mayor concentración de nodos, dado que es el lugar de evacuación en caso de incidencias. Para el primer y segundo piso se ha considerado 30% de nodos en cada planta.

La característica principal de las redes robustas es que pueden percibir en forma inmediata los cambios topológicos o daños en sus nodos, esto ha permitido su uso y aplicación en situaciones de emergencia e incluso ante posibles catástrofes. Para este trabajo se han diseñado tres escenarios que varían en términos de número de nodos (pequeño, mediano y grande) y su ubicación o distribución en el edificio. La idea de éste diseño e implementación es comprobar la robustez de una red de sensores sometida a condiciones de emergencias inesperadas, tal como se muestra en la Tabla I. Cabe mencionar que las pruebas se realizaron de forma dinámica, es decir la topología de la red dentro de la simulación son variables, es decir, en un determinado momento ciertos nodos permanecían activos mientras que aleatoriamente se apagaban cierto porcentaje de nodos (dependiendo del escenario), haciendo que se realice una reconfiguración de la red y por

ende un cambio en la topología, es por ello que queda implícito el hecho de manejar una topología de red dinámica y no disponer de un gráfico que permita describir la topología de forma general.

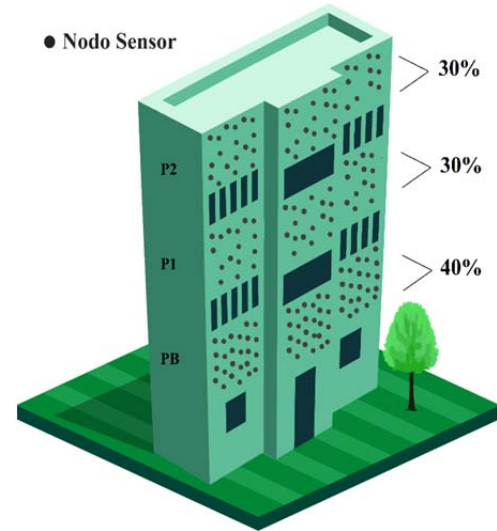


Fig. 3 Modelo de edificio con dispersión y proporción de nodos sensores por pisos planteado para la simulación de robustez

TABLA I. DISTRIBUCIÓN DE LA CANTIDAD DE NODOS EN LOS DISTINTOS

Planta	Escenario / Cantidad de nodos		
	Pequeño	Mediano	Grande
PB	20	100	200
P1	15	75	150
P2	15	75	150
Total de Nodos:	50	250	500

ESCENARIOS DE SIMULACIÓN

Los nodos sensores se encuentran ubicados alrededor de cada piso de acuerdo a coordenadas fijas. Durante la realización de las pruebas, el sistema es sometido a pérdidas de nodos, lo que permite realizar el análisis de enrutamiento de los protocolos simulados. La densidad de nodos apagados se establece en términos de la pérdida de nodos, como se evidencia en la Tabla II.

% Pérdida de Nodos	Cantidad Nodos / Escenario		
	Grande	Mediano	Pequeño
10	50	25	5
30	150	75	15
60	300	150	30

TABLA II. CANTIDAD DE NODOS PERDIDOS POR ESCENARIOS

Los protocolos de enrutamiento aseguran el direccionamiento de los paquetes a sus destinos, enviándolos a través del Protocolo de Datagrama de Usuario (UDP). No obstante, el tiempo que le toma al sistema generar un mensaje de verificación indicando que los datos están correctos es

% Pérdida de Nodos	Cantidad de Nodos / Planta del Edificio		
	PB	P1	P2
10	0	0	50
30	0	75	75
60	100	100	100

considerable, por lo que es recomendable usar un procesador veloz y con capacidad suficiente de memoria para evitar latencias altas. Una vez que se tiene diseñada la red de sensores, es necesario seleccionar el protocolo de enrutamiento proactivo que mejore desempeño de la misma. En la Tabla III [7][8], el

Parámetros	Valores
Plataforma de Simulación	Ubuntu 14.04 Procesador AMD-64 2.4Ghz, 6Gb RAM
Simulador	NS3.23
Tiempo Simulación	900 s
Tamaño Paquete	128 bytes
Frecuencia de Envío	314 us
Tiempo Apagado Nodos	720 s
Tipo Tráfico	UDP

número de nodos y porcentaje de pérdida considerados para las simulaciones de cada protocolo en NS3 en base a los escenarios definidos.

TABLA III. ESPECIFICACIONES DE LA SIMULACIÓN

Durante la simulación se generan archivos de extensión “.pcap”, que son visualizados por medio del programa Wireshark. Estos archivos contienen datos para cálculos de retardo, variación del retardo, número de paquetes enviados y recibidos de cada uno de los nodos sensores hacia su destino. En base a estos resultados, se obtienen métricas de robustez para el análisis de rendimiento, retardo promedio y pérdida de paquetes que han tenido cada uno de los nodos evaluados [9].

Para elegir el protocolo de enrutamiento proactivo de mejor rendimiento, se han determinado los siguientes parámetros: porcentaje de pérdida de nodos y la cantidad de nodos

% Pérdida de Nodos	Cantidad de Nodos / Planta del Edificio		
	PB	P1	P2
10	0	0	5
30	0	7	8
60	10	10	10

apagados, que son usados para comparar el desempeño de los protocolos para los escenarios propuestos. Esto puede evidenciarse en las tablas IV, V, VI a continuación:

% Pérdida de Nodos	Cantidad de Nodos / Planta del Edificio		
	PB	P1	P2
10	0	0	25
30	0	37	38
60	50	50	50

TABLA IV. DISTRIBUCIÓN DE LA CANTIDAD DE NODOS PERDIDOS – ESCENARIO PEQUEÑO (50 NODOS)

TABLA V. DISTRIBUCIÓN DE LA CANTIDAD DE NODOS PERDIDOS – ESCENARIO MEDIANO (250 NODOS)

TABLA VI. DISTRIBUCIÓN DE LA CANTIDAD DE NODOS PERDIDOS – ESCENARIO GRANDE (500 NODOS)

Para la implementación del entorno de simulación se han definido los siguientes criterios:

- *Nodo Sumidero*: Nodo de estación base ubicado en la planta baja del edificio, mismo que recibe la información de estado de todos los nodos sensores.
- *Nodo Evaluado*: Son nodos sensores cercanos a los nodos que fueron apagados durante la simulación, luego son analizados para determinar la robustez del protocolo.
- *Distribución de Nodos*: Cada nodo esta numerado para el análisis de robustez, con esto se puede identificar rápidamente por medio del número del nodo sensor, cual planta del edificio ha sido afectada, tal como se observa en la Tabla VII.

Planta	Escenario / Numeración de Nodos		
	Pequeño	Mediano	Grande
PB	1-20	1-100	1-200
P1	21-35	101-175	201-350
P2	36-50	176-250	351-500
Total de Nodos:	50	250	500

TABLA VII. DISTRIBUCIÓN DE LOS NODOS ENUMERADOS

- *Pérdida de Nodos*: Los nodos sensores son divididos en 3 grupos de acuerdo a su posición con respecto al nodo sumidero. Así, el grupo de nodos cercanos, medianos y lejanos, se encuentran ubicados en la planta baja, primer piso y segundo piso respectivamente. El apagado de estos nodos sensores depende de los porcentajes de pérdida en cada escenario.

TABLA VIII. ETIQUETAS DE NODOS EVALUADOS EN ESCENARIO PEQUEÑO (50 NODOS)

% Pérdida de Nodos	Nº Nodos Evaluados / Planta del Edificio		
	PB	P1	P2
10	-	-	41, 42, 44, 47, 50
30	-	28, 29	43, 44, 47
60	11	31, 32	49, 50

TABLA IX. ETIQUETAS DE NODOS EVALUADOS EN ESCENARIO MEDIANO (250 NODOS)

% Pérdida de Nodos	Nº Nodos Evaluados / Planta del Edificio		
	PB	P1	P2
10	-	-	244, 246, 247, 248, 250
30	-	138, 144	240, 244, 250
60	80	163, 172	249, 250

% Pérdida de Nodos	Nº Nodos Evaluados / Planta del Edificio		
	PB	P1	P2
10	-	-	461, 462, 468, 470, 450
30	-	278, 279	443, 444, 447
60	101	301, 302	451, 500

TABLA X. ETIQUETAS DE NODOS EVALUADOS EN ESCENARIO GRANDE (500 NODOS)

A. Método de evaluación

Se ha considerado la distancia entre los nodos sensores hacia el nodo sumidero, como el método principal para evaluar la robustez del protocolo de enrutamiento. Por lo cual, se ha establecido al primer y segundo piso con mayor porcentaje de pérdida de nodos para los casos de 10% y 30%, debido a que el nodo sumidero se encuentra en la planta baja. En el último porcentaje de pérdida de 60%, se ha distribuido equitativamente dicho porcentaje para todos los pisos del edificio.

Mientras se ejecuta la simulación de cada uno de los escenarios dentro de la red de sensores, se seleccionan los nodos evaluados, los mismos que son utilizados para obtener datos relevantes en el análisis del protocolo de enrutamiento.

B. Criterios de evaluación

Entre los problemas que siempre presentan las redes de sensores están el exceso de memoria en sus búferes, contención de canales, congestión provocando pérdida de paquete, retardos y alto consumo en procesos de control. Por tanto, los criterios a considerar en los escenarios son: *el tiempo de rendimiento promedio que tienen los nodos evaluados durante la simulación, el retardo promedio en términos de latencia que experimenta el sistema de sensores y el porcentaje de pérdida de paquetes.*

IV. PRUEBAS Y ANALISIS DE RESULTADOS

A. Pruebas de Rendimiento

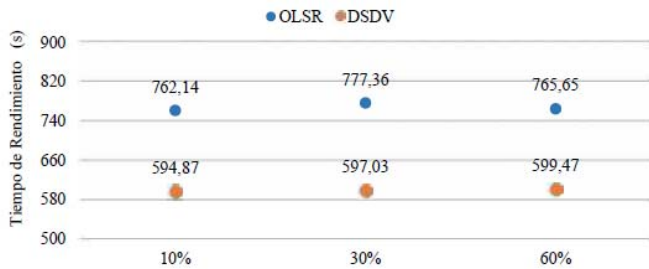


Fig. 4 Tiempo de rendimiento promedio de Nodos Evaluados por Porcentaje de pérdidas en el Escenario Pequeño

En la Fig. 4, se muestran los tiempos que el nodo sumidero dejó de recibir respuesta por parte de los nodos evaluados. Para este escenario se simulan 50 nodos y los resultados revelan que, para cada uno de los porcentajes de pérdida considerados, el protocolo OLSR tiene un mayor tiempo de rendimiento promedio.

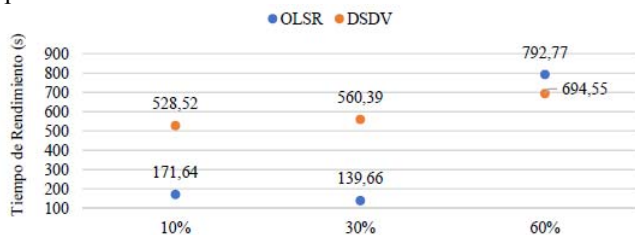


Fig. 5 Tiempo de rendimiento promedio de Nodos Evaluados por Porcentaje de pérdidas en el Escenario Mediano

En la Fig. 5 se puede observar que el protocolo DSDV obtiene el mayor tiempo de rendimiento cuando los porcentajes de pérdida corresponden 10% y 30%. Para el último porcentaje de caída, el protocolo OLSR resiste más tiempo llegando a funcionar casi 793 segundos. Sin embargo, los tiempos de rendimiento promedio no tuvieron concordancia debido a que para las pérdidas de 10% y 30% los tiempos fueron muy bajos comparados a los que se obtuvo en el caso más crítico de pérdida de nodos.

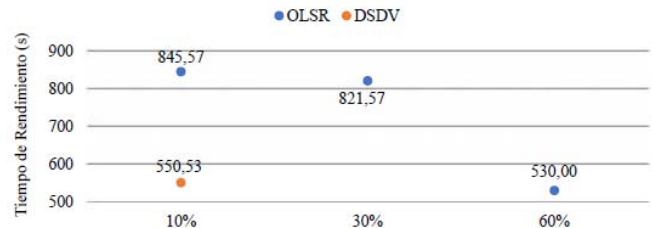


Fig. 6 Tiempo de rendimiento promedio de Nodos Evaluados por Porcentaje de pérdidas en el Escenario Grande

Para este último escenario descrito en la Fig. 6, se observa que en los porcentajes de pérdida de 30 y 60%, el tiempo de rendimiento promedio correspondiente al protocolo DSDV es de 0 debido a que no soporta la simulación con esta densidad de nodos después de las pérdidas respectivas. Para este caso en particular, no se considera la generación de mensajes UDP y la actualización de las tablas de enrutamiento correspondientes a cada nodo. Por el contrario, el protocolo OLSR soporta la simulación de 500 nodos para los diferentes porcentajes de pérdidas, teniendo un mayor tiempo de rendimiento en las pérdidas de 10% y 30%. Cuando el análisis sobre el mismo protocolo se realiza considerando un porcentaje de pérdida del 60%, el tiempo de rendimiento es muy bajo debido a la gran caída de nodos que tiene la red de sensores.

B. Pruebas de Robustez

La robustez del protocolo se evalúa distribuyendo un mayor porcentaje de pérdida de nodos entre los pisos uno y dos, a excepción del caso de caída del 10% donde su totalidad de pérdida de nodos se da solo en el segundo piso. De esta forma, se concluye las simulaciones especificadas para cada uno de los escenarios propuestos. Los resultados de las pruebas se muestran en las Fig. 7, 8, 9, 10 y 11, donde se compara los retardos y porcentaje de pérdida de paquetes muestran la comparación que se realiza entre los retardos y porcentaje de pérdida de paquetes promedio que obtuvieron los nodos evaluados en cada protocolo.

- *Escenario Pequeño (50 Nodos)*

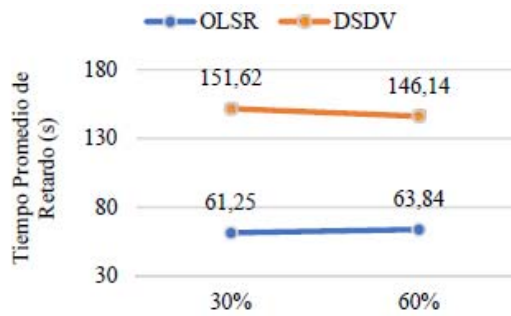


Fig. 7 Retardo Promedio de Nodos Evaluados en el primer piso por Porcentaje de pérdida (No cuenta con pérdida del 10%)

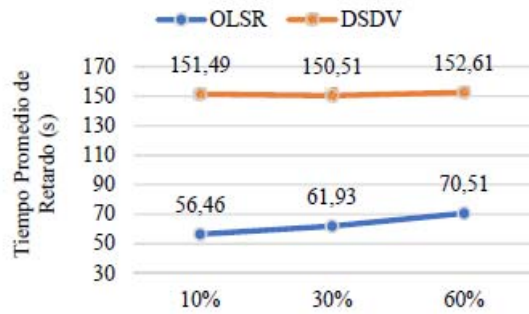


Fig. 8 Retardo Promedio de Nodos Evaluados en el segundo piso por Porcentaje de pérdida

Los retardos promedio de los nodos evaluados determinan el tiempo que les tomó transmitir su estado al sumidero luego de percibir las pérdidas de nodos que tuvo la red. En las Fig. 7 y 8 se observan retardos muy distantes en ambos pisos, teniendo al protocolo OLSR con los menores tiempos de retardo promedio, lo que indica que la caída de los nodos no le afecta tanto en comparación al protocolo DSDV, el cual muestra ¡altos tiempos de retardo promedio.

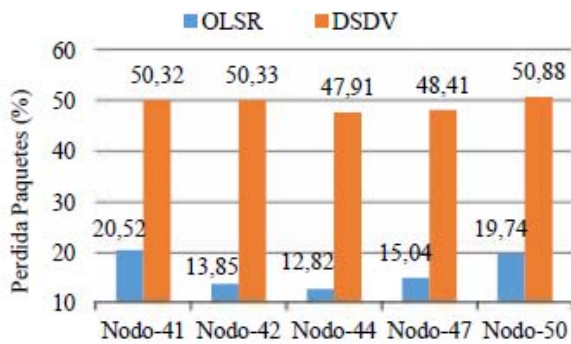


Fig. 9 Porcentaje de pérdida de paquetes en nodos evaluados (Pérdida 10%)

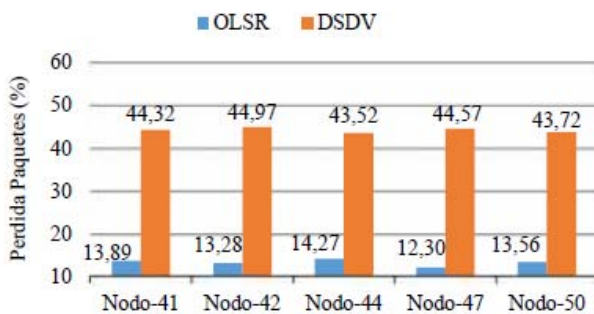


Fig. 10 Porcentaje de pérdida de paquetes en nodos evaluados (Pérdida 30%)

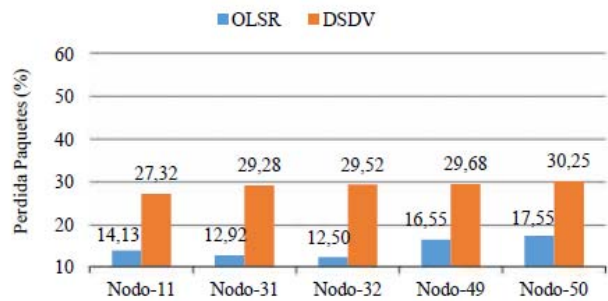


Fig. 11 Porcentaje de pérdida de paquetes en nodos evaluados (Pérdida 60%)

En las Fig. 9, 10 y 11, se muestran los porcentajes de pérdida de paquetes de cada uno de los nodos evaluados por porcentaje de caída de nodos. Para las caídas de nodos de 10% y 30%, los porcentajes de pérdida de paquetes del protocolo DSDV están por arriba de 47,9% y 43,5% respectivamente, valores altos en relación a los obtenidos por OLSR. En el caso de caída de nodos de 60%, los valores de pérdida de nodos correspondientes al protocolo DSDV son casi el doble a los del protocolo OLSR, donde para este último protocolo los porcentajes de pérdida se mantuvieron por debajo de 17,6%.

- *Escenario Mediano (250 Nodos)*

Para este escenario los resultados de los retardos promedio de los nodos evaluados se muestran en las Figuras 12 y 13. En el segundo piso, el protocolo DSDV para los porcentajes de pérdida de 10% y 30% se obtiene retardos promedio significativamente menores comparado a los del protocolo OLSR, mientras que para el porcentaje de pérdida de 60% el retardo promedio del protocolo DSDV es mayor al obtenido por el protocolo OLSR. De igual forma, los resultados de menor retardo promedio en el primer piso para el caso de pérdida de nodos de 30% es de 106,2 segundos correspondiente al protocolo DSDV y para la caída de nodos de 60%, el protocolo OLSR obtuvo un retardo promedio de 294,64 segundos.



Fig. 12 Retardo promedio de nodos evaluados en el primer piso por porcentaje de pérdida (No cuenta con pérdida del 10%)

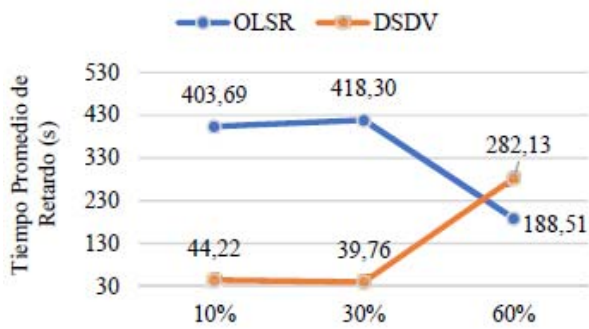


Fig. 13 Retardo promedio de nodos evaluados en el segundo piso por porcentaje de pérdida

En general los porcentajes de pérdida de paquetes promedio en las diferentes caídas de nodos fueron muy altos para ambos protocolos. El protocolo DSDV en todas las caídas de nodos obtiene menores porcentajes de pérdida de paquetes promedio en comparación a los resultados del protocolo OLSR. Sin embargo, los porcentajes de pérdida variaron desde un 48% hasta 74% para los casos de pérdida de 10% y 30%; mientras que para el 60% de caída los porcentajes de pérdida de paquetes de la mayoría de los nodos evaluados del protocolo DSDV estuvieron por arriba del 55%. Los resultados de los nodos evaluados en este escenario son desfavorables, con lo que se concluye que hubo un bajo desempeño de ambos protocolos.

- *Escenario Grande (500 Nodos)*

Para el último escenario de 500 nodos las Fig. 14 y 15, muestran retardos promedio de los nodos evaluados del segundo y primer piso respectivamente. Para las caídas de nodos correspondientes a 30% y 60%, el protocolo DSDV no pudo mantener su funcionamiento debido a esto el retardo es 0. Para la caída de 10% su retardo promedio fue aproximadamente 21 segundos más comparado con el tiempo que obtuvo OLSR bajo el mismo escenario. Por otro lado, OLSR pudo resistir las pruebas con sus respectivas caídas de nodos, sin embargo, los resultados más altos llegaron hasta un 85% promedio de pérdida de paquetes de los nodos evaluados para el caso de 60% de caída.

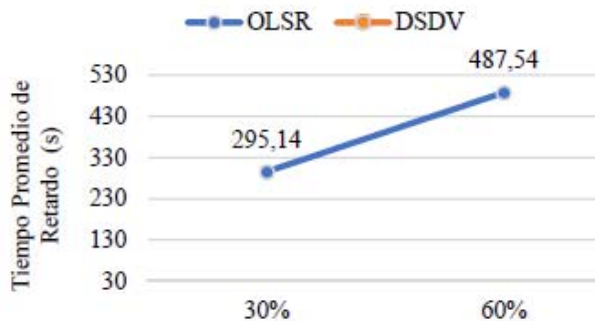


Fig. 14 Retardo Promedio de Nodos Evaluados en el primer piso por Porcentaje de pérdida (No cuenta con pérdida del 10%)

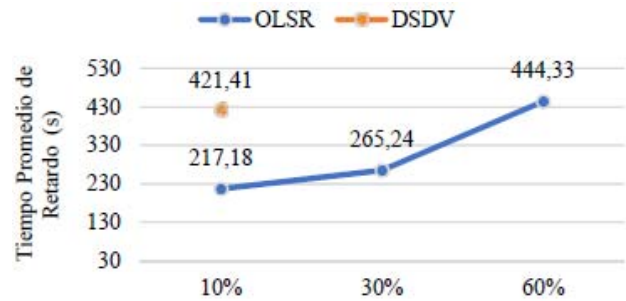


Fig. 15 Retardo Promedio de Nodos Evaluados en el segundo piso por Porcentaje de pérdida

Para calificar el desempeño que han tenido los protocolos de enrutamiento, se ha determinado puntuaciones según los resultados obtenidos en cada uno de los criterios de robustez en las respectivas simulaciones.

Aceptable si los valores de los tiempos de rendimiento promedio de los nodos evaluados se extienden un minuto luego de presentar las respectivas caídas. Además, que los retardos promedio no excedan los 71, 110, 260 segundos dependiendo el tipo de escenario pequeño, mediano y grande respectivamente y los porcentajes de pérdida de paquetes promedio no sean superiores a 30%.

Regular se tiene que los resultados de los tiempos de rendimiento promedio de los nodos evaluados se prolongan 48 segundos luego de la pérdida de nodos, sus retardos promedio llegan hasta 79, 118, 273 segundos de acuerdo al tipo de escenario pequeño, mediano y grande respectivamente y los porcentajes de pérdida de paquetes promedio estén dentro del 31% hasta 45%.

Malo si los resultados de los tiempos de rendimiento promedio de los nodos evaluados no llegan a 720 segundos, los retardos promedio no superan los 89, 137, 295 segundos para cada tipo de escenario pequeño, mediano y grande respectivamente y los porcentajes de pérdida de paquetes promedio se encuentran por encima del 45%.

Pésimo si con las simulaciones realizadas, el protocolo no pudo ser evaluado, debido al no poder establecerse el enrutamiento.

TABLA XI. PRUEBAS DE LAS SIMULACIÓN CON VALORACIONES SEGÚN LOS CRITERIOS DE ROBUSTEZ

Escenarios	Rendimiento		Retardo Promedio		Pérdida de Paquetes	
	OLSR	DSDV	OLSR	DSDV	OLSR	DSDV
Pequeño	R	M	A	M	A	R
Mediano	M	M	M	M	M	M
Grande	R	P	M	P	M	P

La Tabla XI muestra las valoraciones en base a los criterios de robustez que han tenido los protocolos en cada tipo de escenario. Para la simulación mínima de 50 nodos el protocolo OLSR obtuvo mejores puntuaciones en todos los aspectos analizados, siendo el ideal para este tipo de red. En el escenario mediano las valoraciones obtenidas en cada criterio correspondiente al protocolo OLSR son totalmente diferentes al caso anterior, considerando que, si bien las estadísticas de rendimiento de 60% de pérdidas de nodos resultaron mejores

que DSDV, sus retardos y porcentajes de pérdida de paquetes promedio son superiores a los obtenidos por DSDV. En general, los resultados fueron malos para ambos protocolos, por lo tanto, ninguno es adecuado para esta cantidad de nodos. Para el último caso de 500 nodos, el protocolo DSDV únicamente pudo ser simulado con el 10% de pérdida de nodos obteniendo resultados malos, para los otros porcentajes de caída de nodos, dónde incluso el protocolo no pudo ser evaluado debido a la ausencia de paquetes UDP, por lo cual obtuvo una valoración pésima para estos escenarios. El protocolo OLSR tuvo un tiempo de rendimiento promedio valorado como regular, pero sus retardos y porcentajes de pérdida de paquetes promedio estuvieron elevados teniendo valoraciones malas, inadecuado para implementarlo en el sistema de sensores cuando ocurra una emergencia considerable.

El análisis realizado determina que el protocolo OLSR puede ser implementado tanto en redes pequeñas como en grandes. El rendimiento en OLSR es robusto, dado que se mantuvo aproximadamente 48 segundos luego de presentar las pérdidas de nodos, en el caso de 60% de pérdida de nodos cuando se simuló una red grande, los resultados de retardos y porcentajes de pérdida de paquetes promedio tuvieron valoraciones malas mientras que en el caso del escenario mediano los resultados de los nodos evaluados fueron malos en relación a cada uno de los criterios de robustez

V. CONCLUSIONES

La importancia al distribuir los nodos sensores en diferentes posiciones en cada piso y utilizar el método basado en la distancia entre los sensores como principal aspecto para establecer la robustez de un sistema, facilita la simulación de grandes redes. A esto, la arbitrariedad de elegir condiciones específicas, las mismas que hacen posible que el análisis realizado sea más adaptable a la realidad. El protocolo de enrutamiento proactivo OLSR, presenta un mejor desempeño en todos los aspectos de robustez bajo las especificaciones y escenarios considerados en este trabajo, lo que abre un sin número de posibles simulaciones que pueden realizarse para analizar otros protocolos de enrutamiento proactivos, incluso el poder hacer la comparación con protocolos reactivos tales como: Ad hoc On-Demand Distance Vector (AODV), y apreciar el desempeño en situaciones de emergencias. Un punto necesario a considerar es el tamaño de los paquetes que se van a enviar a la red, es por ello que como trabajo futuro se podría plantear un estudio en base a ello para determinar si hay variación en el rendimiento de cada uno de los protocolos analizados en este tipo de aplicaciones.

En base a la investigación realizada se concluye que, sin importar el escenario simulado, para los casos de emergencia donde el daño de los nodos es inferior al 40%, se debe considerar el protocolo OLSR para la implementación del sistema de sensores, “si sólo se considera los protocolos proactivos”.

AGRADECIMIENTO

Un agradecimiento especial al Laboratorio de Sistemas Distribuidos de la Escuela Superior Politécnica del Litoral, por ofrecer un ambiente adecuado (Servidores) para la ejecución de las simulaciones, permitiendo continuar con el proyecto KISHUAR.

REFERENCIAS

- [1] Munoz, J. A., Calero, V., Marin, I., Chavez, P., & Perez, R. (2015). Adaptive evacuation management system based on monitoring techniques. *IEEE Latin America Transactions*, 13(11), 3621-3626.
- [2] Munoz-Arcatales, Andres, Wendy Yáñez-Pazmino, and Washington Velásquez Vargas. "Proposal of a communication structure model for activating reactive signaling in an emergency evacuation systems." *Computing and Communication Workshop and Conference (CCWC), 2017 IEEE 7th Annual*. IEEE, 2017.
- [3] Vargas, Washington Velásquez, Andres Munoz-Arcatales, and Joaquín Salvachúa Rodríguez. "A distributed system model for managing data ingestion in a wireless sensor network." *Computing and Communication Workshop and Conference (CCWC), 2017 IEEE 7th Annual*. IEEE, 2017.
- [4] Jianli Pan, Raj Jain, "A Survey of Network Simulation Tools: Current Status and Future Development", Washington University in St. Louis School of Engineering & Applied Science, Department of Computer Science & Engineering, 2008.
- [5] Romana Rahman Ema, Ashrafi Akram, Md. Alam Hossain, Subrata Kumar Das, "Performance Analysis of DSDV, AODV AND AOMDV Routing Protocols based on Fixed and Mobility Network Model in Wireless Sensor Network", *Global Journal of Computer Science and Technology: E, Network, Web & Security*, Volume 14 Issue 6 Version 1.0, 2014.
- [6] Aron Laszka, Levente Buttyán, Dávid Szeszlér, "Designing robust network topologies for wireless sensor networks in adversarial environments", Department of Telecommunications, Department of Computer Science and Information Theory, Budapest University of Technology and Economics, 2013.
- [7] C.Jeyalakshmi, R.Sukumar, "An Experimental Study on Optimized Link State Routing Protocol for Underground Mines", *Int.J.Computer Technology & Applications*, Vol 3, 2012.
- [8] Yu-Dong Tan, Xiao-Qin Huang, Ye Cai, Yi Tan, and An-Gang Chen, "Design of Wireless Sensor Networks Considering the Robustness of the topology", College of Electrical and Information Engineering, Hunan University, ChangSha, 410082 Hunan Province, China, 2012.
- [9] Ayakumar T.P, N. Gunasekaran, "Empirical Factors for Robustness of Sensor Nodes on Energy Efficiency", *Recent Advances in Computer Engineering, Communications and Information Technology*, 2013.
- [10] Vatsalya Kunchakarra, "Simulation Study of Routing Protocols in Wireless Sensor Networks", Faculty of the Louisiana State University and Agricultural and Mechanical College, Louisiana, EEUU, December 2005.
- [11] Aron Laszka, Levente Buttyán, Dávid Szeszlér, "Designing robust network topologies for wireless sensor networks in adversarial environments", Department of Telecommunications, Department of Computer Science and Information Theory, Budapest University of Technology and Economics, 2013.
- [12] C.Jeyalakshmi, R.Sukumar, "An Experimental Study on Optimized Link State Routing Protocol for Underground Mines", *Int.J.Computer Technology & Applications*, Vol 3, 2012.



Roberto Cordova Estrella (Guayaquil – Ecuador). He was graduated as Telematics Engineer on 2016 (ESPOL, Ecuador). He is currently working in a telecommunication company.

Madrid since October 2016 in Telemetry and Remote Control in Emergencies.



Ignacio Marin-Garcia (Logroño - Spain, 1975). He received his bachelor in Science Engineering Technology degree in 2003 and his Master Science in Information Systems in 2006, both from Northeastern University. He currently works as Full-time assistant professor at Telematics Engineering department at Escuela Superior Politécnica del Litoral (ESPOL). His research interests include HPC, VLC, virtualization, security and education. He has been member of ACM since 2004 and IEEE since 2003 (computer society and standard association). HE worked as a Junior Researcher and Teaching Assistant at the “ITEST Robotics” project (NSF 0423059).



Jose Andrés Muñoz-Arcentales (Santo Domingo - Ecuador, 1989). He was graduated as Telematics Engineer on 2013 (ESPOL, Ecuador). He has worked as Assistant Professor of Telematic's Department since 2013 at Escuela Superior Politécnica del Litoral. He has been researching in fields like, Visible Light Communications, Smart Farming and Reactive Evacuation Systems with a major research interest in Sensor Networks and Embedded Systems. He was graduated as master in Redes y Servicios Telemáticos at Universidad Politécnica de Madrid.



Victor Asanza is a student of the Doctorate in Applied Computational Sciences and a research at the Information Technology Center, at the Escuela Superior Politécnica del Litoral, Ecuador. Since 2014, I have been involved in the application of artificial intelligence algorithms with temporary signals.



Washington A. Velásquez Vargas (Guayaquil - Ecuador, 1988). He was graduated as Telematics Engineer on 2013 (ESPOL, Ecuador). He has worked as Professor of Telematic's Department since 2014 at Escuela Superior Politécnica del Litoral. He has been researching in fields like, Telemetry and Remote Control, Smart Cities and Big data with a major research interest in Telemedicine and Embedded Systems. Currently, He is Ph.D. Candidate at Universidad Politécnica de