PROYECTO FIN DE MÁSTER EN

SISTEMAS INTELIGENTES

CURSO 2008-2009

PROTOCOLO DE ENCAMINAMIENTO PARA REDES INALÁMBRICAS DE SENSORES EN APLICACIONES DE MONITOREO Y CONTROL

Nelson Javier Cárdenas Parra

Director:

Alfredo Fernández-Valmayor Crespo

Departamento de Ingeniería del Software e Inteligencia Artificial

Colaborador externo de dirección:

Luis Javier García Villalba

Departamento de Ingeniería del Software e Inteligencia Artificial

---

MÁSTER EN INVESTIGACIÓN EN INFORMÁTICA

FACULTAD DE INFORMÁTICA

UNIVERSIDAD COMPLUTENSE DE MADRID

El abajo firmante, matriculado en el Máster en Investigación en Informática de la Facultad de Informática, autoriza a la Universidad Complutense de Madrid (UCM) a difundir y utilizar con fines académicos, no comerciales y mencionando expresamente a su autor el presente Trabajo Fin de Máster: ”Protocolo de Encaminamiento para Redes Inalámbricas de Sensores en Aplicaciones de Monitoreo y Control”, realizado durante el curso académico 2008-2009 bajo la dirección de Alfredo Fernández-Valmayor Crespo y con la colaboración externa de dirección de Luis Javier García Villalba en el Departamento de Ingenieria del Software e Inteligencia Artificial, y a la Biblioteca de la UCM a depositarlo en el Archivo Institucional E-Prints Complutense con el objeto de incrementar la difusión, uso e impacto del trabajo en Internet y garantizar su preservación y acceso a largo plazo.

Nelson Javier Cárdenas Parra

Abstract

Reduction in size and cost of sensor devices have incremented their use to monitoring specific environments without periodic supervision. Each node in a wireless sensor network has limited resources but using communication and cooperative processing strategies the network in a distributive way can do application tasks. The main goal of many wireless sensor applications consist in send collected information from a specific area to a central point or base station for later processing.

During our study of wireless sensor networks protocols, we had found different proposals concerning in message reliability and energy saving. However, during this study, we have not found a protocol that correlate interest metrics, for this application type, as: energy saving, link quality and data aggregation and the same time correlate these three aspects with message reliability.

In this work is proposed a wireless sensor network routing protocol concern in message reliability and energy saving. Considering aspects as available energy, link quality, number of hops and data communication criteria. Additionally also contributes to network lifetime, coverage and effective sampling rate. *SHRP* protocol support very common but unpredictable changes in network topology. Using Simulation we analyze the throughput of proposal protocol and compare it with a similar protocol in different scenarios in order to show its advantages

Keywords: 802.15.4, routing protocol, wireless sensor network

Resumen

La reducción en el tamaño y en el costo de dispositivos sensores ha incrementado su uso para monitorear ambientes específicos sin la necesidad de supervisión periódica. Cada nodo en una red de sensores inalámbricos posee recursos limitados, pero a través de estrategias de comunicación y procesamiento cooperativo le permite a la red de forma distribuida realizar las tareas de la aplicación. Muchas de las aplicaciones de redes de sensores buscan hacer llegar la información recolectada en un área específica de interés a un punto central o estación base para su procesamiento.

Al evaluar los protocolos de encaminamiento para redes de sensores encontramos distintas propuestas que ofrecen confiabilidad en la entrega de mensajes y ahorro de energía. Sin embargo, durante el estudio realizado, no se ha encontrado un protocolo que correlacione las métricas de interés para este tipo de aplicaciones, como lo son: ahorro de energía, calidad de enlace y agregación de datos, y que a su vez asocie estos tres aspectos con la confiabilidad en la entrega de los mensajes.

En este trabajo se propone un protocolo de encaminamiento para redes inalámbricas de sensores que toma en cuenta tanto la confiabilidad en la entrega de los mensajes como en el ahorro de energía. Para ello considera aspectos como: batería aún disponible, calidad del enlace, cantidad de saltos hasta el destino y criterios de transmisión de datos. Adicionalmente, al considerar estas métricas, también se contribuye con el tiempo de vida, la cobertura y la tasa de muestreo efectiva. *SHRP* es un protocolo que soporta los cambios impredecibles pero comunes en la topología de la red. Utilizando modelos de simulación se analiza el desempeño del protocolo propuesto y se compara con otro protocolo similar en diversos escenarios para mostrar sus ventajas.

Palabras clave: redes de sensores, Protocolos de encaminamiento, IEEE 802.15.4

Índice general

1. Introducción **1**

1.1. Caso de Estudio 3

1.2. Objetivos 5

2. Planteamiento del problema **7**

2.1. Arquitectura de las Redes Inalámbricas de Sensores 7

2.1.1. Nodos Sensores o Motes 8

2.1.2. Estación Base o SINK 10

2.1.3. Gateways para RIS 11

2.2. Protocolos de Encaminamiento: Restricciones y Retos 11

2.3. Características de las Aplicaciones de Monitoreo que usan WSN 13

2.4. Aspectos a Considerar por los Protocolos de Encaminamiento para Aplicaciones de Monitoreo 15

2.5. Soluciones Relacionadas con las Métricas de Interés 15

3. Trabajos Relacionados **18**

3.1. Protocolos Planos 19

3.1.1. Inundación 19

3.1.2. Fidelidad Adaptativa Geográfica 20

3.1.3. SPIN (Sensor Protocol for Information via Negotiation) 20

3.1.4. Directed Diffusion 21
3.2. Protocolos Jerárquicos 23
3.2.1. LEACH 23
3.2.2. TEEN 24
3.2.3. SAR 25
3.2.4. DIRq 26

4. Solución Propuesta **27**
4.1. Arquitectura 27
4.2. Funciones de los Nodos 30
4.2.1. Nodo Sensor (SN) 30
4.2.2. Nodo Coordinador (CN) 30
4.2.3. Nodo Sink 30
4.3. Configuración de la Topología 31
4.4. Mensajes SHRP 32
4.4.1. Encabezado SHRP 32
4.4.2. Mensaje de Informacion de la Red (NMI) 34
4.4.3. Mensaje Hello 36
4.4.4. Alarmas 38
4.4.5. Mensajes de Datos 39
4.5. Métricas usadas por SHRP 39
4.5.1. Batería Disponible 40
4.5.2. Número de saltos 40
4.5.3. Calidad de Enlace 40
4.5.4. Cálculo de las métricas 42

4.5.5. Umbrales Utilizados 43
4.6. Selección del camino 43
4.6.1. Información de los vecinos 43
4.6.2. Criterio de Selección 48

5. Resultados experimentales **49**
5.1. Selección de la Herramienta para la simulación de Redes Inalámbricas de Sensores 50
5.2. NS-2 51
5.3. Metodología 52
5.4. Entorno de Simulación 55
5.5. Experimentos Realizados 57
5.6. Resultados 72

6. Conclusiones y Trabajo Futuro **78**
6.1. Conclusiones 78
6.2. Trabajo Futuro 79

Apéndices **87**

A. La Tecnología IEEE 802.15.4 **88**
A.1. Objetivos 88
A.2. Componentes de una red IEEE-802.15.4 89
A.3. Topologías de Red 90
A.4. Arquitectura del estándar IEEE-802.15.4 91
A.4.1. Capa de Acceso al Medio (MAC) 93

B. Redes Inalámbricas de Sensores **95**

B.1. Características comunes de las Redes Inalámbricas de Sensores (RIS) . . 96

B.2. Modelo Funcional para las Redes de Sensores 97

B.3. Clasificación de las Aplicaciones para Redes de Sensores 98

B.3.1. Monitoreo y Control 98

B.3.2. Seguridad 100

B.3.3. Seguimiento o Rastreo 101

B.3.4. Redes Híbridas 101

B.3.5. Redes Centradas en los Datos 102

B.4. Métricas de Evaluación de las Redes de Sensores 102

B.4.1. Costo y facilidad de despliegue 103

B.4.2. Cobertura 104

B.4.3. Tiempo de Vida 104

B.4.4. Tasa de Muestreo Efectiva 105

B.4.5. Precisión temporal 106

B.4.6. Tiempo de Respuesta 106

B.4.7. Seguridad 107

C. Herramientas de Simulación para Redes inalámbricas de Sensores **108**

C.1. Sensorsim [44] 109

C.2. Squalnet [47] 110

C.3. SENSE [43] 111

C.4. Mannasim [29] 112

C.5. Vmnet [54] 114

C.6. Truetime [52] 115

C.7. PowerTOSSIM 115

Índice de tablas

5.1. Variables utilizadas en el Entorno de Simulación 55

5.2. Parámetros de Configuración Específicos para *SHRP* y *Directed Diffusion* 57

5.3. Cantidad de Mensajes Enviados en cada experimento 60

5.4. Suma de los Mensajes de Control y de Datos Descartados en cada experimento 68

5.5. Promedio de Bateria Disponible y Desviación Stándar para cada Experimento 71

Índice de figuras

2.1. Mote MicaZ: tamaño(mm): 58x32x7 peso (gramos): 18 (Sin baterías) . . . 9

4.1. Formato del Encabezado de los Mensajes 33

4.2. Formato del mensaje NMI 34

4.3. Formato del mensaje Hello 37

4.4. Ejemplos de topologías para ilustrar las estrategias en el manejo del mensaje Hello 38

4.5. Ejemplo de una conformación de topología, se indican los valores de batería disponibles en cada nodo 46

4.6. Múltiples caminos válidos para alcanzar Sink desde un nodo K, con distintos números de saltos 47

5.1. Ejemplo del tipo de topología en forma de malla utilizada en los experimentos 56

5.2. Comparación de los mensajes transmitidos por *SHRP* y *Directed Diffusion* para 10 nodos 58

5.3. Comparación de los mensajes transmitidos por *SHRP* y *Directed Diffusion* para 20 nodos 59

5.4. Comparación de los mensajes transmitidos por *SHRP* y *Directed Diffusion* para 50 nodos 61

5.5. Comparación de los mensajes transmitidos por *SHRP* y *Directed Diffusion* para 100 nodos 62

5.6. Comparación de los mensajes descartados por *SHRP* y *Directed Diffusion* para 10 nodos 64

5.7. Comparación de los mensajes descartados por *SHRP* y *Directed Diffusion* para 20 nodos 65

5.8. Comparación de los mensajes descartados por *SHRP* y *Directed Diffusion* para 50 nodos 66

5.9. Comparación de los mensajes descartados por *SHRP* y *Directed Diffusion* para 100 nodos 67

5.10. Comparación de los mensajes enviados por *SHRP* y *Directed Diffusion* para 50 nodos con Mínima energía disponible 69

5.11. Comparación de los mensajes descartados por *SHRP* y *Directed Diffusion* para 50 nodos con Mínima energía disponible 70

5.12. Comparación del consumo de bateria utilizando *SHRP* y *Directed Diffusion* para 10 nodos 73

5.13. Comparación del consumo de bateria utilizando *SHRP* y *Directed Diffusion* para 20 nodos 74

5.14. Comparación del consumo de bateria utilizando *SHRP* y *Directed Diffusion* para 50 nodos 75

5.15. Comparación del consumo de bateria utilizando *SHRP* y *Directed Diffusion* para 100 nodos 76

A.1. Ejemplos de topologías estrella y peer-to-peer 90

A.2. Diagrama de las capas ofrecidas por IEEE-802.15.4 91

A.3. Supertrama de sincronización por tiempo en la capa MAC 94

Capítulo 1

Introducción

Toda actividad productiva requiere de un continuo monitoreo y control. En las plantas industriales es necesario vigilar el correcto funcionamiento de motores, bombas y válvulas, por sólo mencionar algunos ejemplos. En el área de seguridad, detectores de movimiento son instalados en las zonas de mayor riesgo o importancia para la organización. En la actualidad, muchas empresas tienen personal asignado para monitorear situaciones críticas.

Durante la última década han aparecido infinidad de dispositivos que utilizan sensores para el monitoreo y control. Las Redes Inalámbricas de Sensores o RIS (también llamadas WSN por sus siglas en inglés) pueden estar compuestos por decenas, cientos o incluso miles de pequeños computadores que operan con baterías, llamados *motes* y que son distribuidos a lo largo de un ambiente de interés particular. Cada nodo en una red ad-hoc recolecta datos de su ambiente, como la cantidad de luz, temperatura, humedad, vibraciones y otros factores ambientales. Cada nodo sensor, puede enviar los datos recolectados a sus vecinos, éstos a su vez a sus propios vecinos y así sucesivamente, hasta que la información alcance un destino específico, donde será procesada

por computadores más "tradicionales", brindando una buena imagen del ambiente circundante en tiempo real [22].

El uso de las redes inalámbricas de sensores comprende aplicaciones muy diversas. Se crearon inicialmente para aplicaciones militares que permitían comunicación y vigilancia ad-hoc. En la actualidad se pueden mencionar aplicaciones de monitoreo industrial, ambiental, agrícola, para el seguimiento de animales en su hábitat, para el control de la operación de equipos, para verificar las propiedades físicas de piezas críticas, entre otros [41].

Por las restricciones que imponen las RIS, las tecnologías que la implementan y las necesidades específicas de las aplicaciones, se requieren protocolos de encaminamiento más eficientes que incluyan criterios como maximizar el tiempo de vida de la red, garantizar la conectividad entre los nodos, lograr una alta tasa de recepción, manejar cambios dinámicos de la topología, etc. Estos protocolos son diseñados con premisas muy diferentes en cuanto a la composición o capas de la red, por lo que protocolos tradicionales basados en IP no pueden ser aplicados a las RIS. Todo esto ha potenciando la investigación en esta área, para buscar nuevas técnicas que eliminen las ineficiencias en el consumo de energía que acortan la vida de la red.

Para describir y ejemplificar el problema se presentará a continuación un ejemplo real que nos permitirá ilustrar las necesidades de una aplicación de monitoreo, usando redes inalámbricas de sensores. Para ello, se ha trabajado conjuntamente con la Fundación de Inversigación y Desarrollo de la Universidad Simón Bolívar en Caracas Venezuela (FUNINDES) quienes están desarrollando un proyecto con Petroleos de Venezuela (PDVSA) y en el que tienen planificado utilizar sensores inalambricos como parte de su propuesta de solución.

1.1. Caso de Estudio

Como parte del proyecto Funindes-PDVSA 32-1899 titulado *Aplicaciones de Tecnologías Relacionadas a Redes Inalámbricas de Sensores en el Negocio de Petróleo y Gas* se requiere recolectar información de la operación de los pozos de petróleo de baja producción, con el fin de aumentar su vida útil, reducir sus costos de operación y mantenimiento, y tomar medidas proactivas al identificar valores que están fuera de sus rangos normales de operación. Esto permitirá reducir las ocurrencias de eventos que puedan disminuir la producción del pozo, o incluso llegar a comprometer tanto al pozo como al yacimiento en el cual se encuentran.

El objetivo del proyecto, consiste en capturar una serie de parámetros que permitan determinar cuál es el comportamiento del pozo, principalmente en cuanto al volumen de petróleo que se extrae. Para estimar éste y otros valores, se miden principalmente la temperatura y presión del petróleo en diferentes lugares del pozo. El almacenamiento de los datos recolectados y su posterior análisis permitirá estimar tendencias de los parámetros medidos por pozo, características del yacimiento, estadísticas de producción y comportamiento periódico del pozo. Estas actividades escapan de la competencia del personal de mantenimiento del pozo, pero son de gran utilidad para determinar estrategias, tanto a nivel operacional como de mantenimiento.

PDVSA ya ha realizado estudios previos para conocer la composición y estructura de sus diferentes tipos de pozos. De dichos estudios se obtuvieron los siguientes aspectos: métodos de producción utilizados, tipos de instalaciones que poseen, materiales con los que están fabricados y las distancias que están involucradas. Una lista inicial de las características y/o restricciones que deben ser tomadas en cuenta al instalar los

sensores son:

- El área que comprende este tipo de pozos donde se colocarán los nodos sensores es relativamente pequeña, máximo 30 metros. Sin embargo, pueden ser múltiples los puntos de medición requeridos.
- Hay que considerar posibles interferencias generadas por los materiales con los que están hechas las tuberías.
- Quizás no habrá línea de vista entre dos dispositivos que estén midiendo valores.
- Los sensores estarán colocados a nivel de la superficie.
- La frecuencia con la que se recolectarán los datos y se enviarán a la estación central será, a lo sumo, cada dos minutos.
- Los pozos se encuentran ubicados en sitios apartados, sin poblaciones cercanas y sin personal permanente. Esto trae como consecuencia que los pozos sean víctimas de la delincuencia para extraer materiales y equipos que puedan luego revender.
- La inversión a realizarse en la instalación y mantenimiento de la infraestructura necesaria para la red debe considerar que se trata de pozos de baja producción (baja rentabilidad) asi como los riesgos descritos en el punto anterior.

Dadas estas restricciones se ha decidido utilizar pequeños dispositivos sensores inalámbricos, llamados motes, para la recolección y transmisión de los datos del pozo. Dicha escogencia se debe, además de su bajo costo, porque instalar una red cableada

es inviable en estos ambientes. Internamente, los motes utilizan la tecnología IEEE-802.15.4 que se ha convertido en un estándar de facto para este tipo de dispositivos.

Aplicaciones de monitoreo como ésta requieren, por una parte, la gestión confiable de los datos periódicos, y por otra parte, la rápida notificación en caso de ocurrir alarmas. El manejo de estos dos tipos de mensajes debe ser bien diferenciado.

Otra consecuencia directa de la topología que se requiere en este caso es la necesidad de un protocolo de encaminamiento de múltiples saltos, ya que a pesar de que las distancias a cubrir son cortas, existe la posibilidad que no haya comunicación directa entre los nodos sensores y la estación base.

No se puede perder de vista que los nodos sensores operan con baterías, así que el ahorro de energía es primordial. Estrategias como la redundancia de mensajes y el envío por múltiples rutas para lograr confiabilidad, quizás pueden causar un consumo extra de energía.

En la actualidad existen propuestas de protocolos de múltiples saltos que ahorran energía. Sin embargo, no se ha encontrado una que cumpla con las necesidades comunes de las aplicaciones de monitoreo, similares a las presentadas en este capítulo, siendo ésta la razón principal que motiva este trabajo de fin de Máster.

1.2. Objetivos

El objetivo de este trabajo es proponer un protocolo de encaminamiento que ofrezca tanto confiabilidad en la recepción de los mensajes como ahorro de energía.

Con esta solución, se busca aumentar el tiempo de vida de la red y al mismo tiempo ofrecer dos características que son importantes para las aplicaciones de monitoreo y control: Primero, establecer rutas confiables para los mensajes que periódicamente enviarán los nodos sensores a la estación base y segundo, que los mensajes de alerta lleguen lo antes posible para tomar las acciones pertinentes.

Para poder cumplir con el objetivo general de este estudio, se plantearon los siguientes objetivos específicos:

1. Diseñar un protocolo de encaminamiento para redes de sensores que tome en consideración las métricas de interés para las aplicaciones de Monitoreo y las correlacione para lograr confiabilidad en la entrega de los mensajes
2. Comparar experimentalmente el protocolo propuesto usando modelos de simulación con el protocolo Directed Diffusion que es uno de los más conocidos en redes de sensores.

Este trabajo se encuentra dividido en 6 capítulos. Posterior a esta introducción, en el capítulo 2 se presentan algunos conceptos necesarios para comprender el problema planteado. En el capítulo 3 se presentan los protocolos estudiados para redes inalámbricas de sensores. Posteriormente, El capítulo 4 explica en detalle la definición del protocolo propuesto. Luego, el capítulo 5 muestra las simulaciones realizadas para estudiar el desempeño del protocolo propuesto y finalmente en el capítulo 6 se presentan las conclusiones y recomendaciones para trabajos futuros.

Capítulo 2

Planteamiento del problema

En este capítulo se presentan los aspectos más importantes que deben estar presentes en un protocolo de encaminamiento para aplicaciones de monitoreo y que permitirán comprender el problema que es estudiado en este trabajo.

En la sección 2.1 se detalla la arquitectura de las redes inalámbricas de sensores, luego en la sección 2.2, se presentan los retos y restricciones que enfrentan los protocolos de encaminamiento para este tipo de redes. En las secciones 2.3 y 2.4 se describen las características de las aplicaciones de monitoreo y los aspectos que deben considerar los protocolos de encaminamiento para este tipo de aplicaciones. Por último, en la sección 2.5, se presentan las soluciones que proponen otros trabajos para responder a cada una de las métricas de interés.

2.1. Arquitectura de las Redes Inalámbricas de Sensores

Las redes inalámbricas de sensores son un conjunto de aplicaciones de redes, enfocadas en permitir la conectividad sin el uso de cables, a sensores y actuadores en

general (i.e. agentes que pueden influir en su entorno) [53]. En una red inalámbrica de sensores, por lo general, los nodos sensores realizan ciertas mediciones, procesan los datos medidos y los transmiten a sus vecinos, que a su vez retransmiten los mensajes a sus vecinos y así sucesivamente hasta que el dato llega a una estación base. Una vez que los datos han llegado a su destino pueden ser procesados y/o almacenados por computadores y aplicaciones mucho más sofisticados [21, 20], obteniendo de esta forma información de la actividad en el área de interés [32].

Definición 2.1 (Red Inalámbrica de Sensores)**.** Una red inalámbrica de sensores es un sistema distribuido que consiste de un gran número de pequeños nodos sensores, esparcidos físicamente, en el área que se desea estudiar para que luego de un proceso de auto organización formen una red inalámbrica ad-hoc [53] y comiencen a transmitir información a los nodos vecinos que le rodean.

A continuación se describen los componentes de la arquitectura de una red inalámbrica de sensores:

2.1.1. Nodos Sensores o Motes

Los nodos sensores por su tamaño frecuentemente son llamados motes. En diccionarios de habla inglesa aparece la palabra Mote definida como: algo pequeño. Una partícula de polvo, que es tan pequeña que es prácticamente imposible de ver [8].

Definición 2.2 (Nodos Sensores)**.** Un nodo sensor (figura 2.1) son dispositivos de computación auto-contenidos que poseen funcionalidades muy básicas en cuanto a sus componentes e interfaces, son generalmente operados con baterías y permiten medir

distintas magnitudes del ambiente que le rodea, como por ejemplo: luz, temperatura, humedad, movimiento, así como realizar acciones bajo ciertas condiciones. Fueron desarrollados originalmente por Intel Research en colaboración con la Universidad de California en Berkeley en el Centro para la Investigación en Tecnologías de la Información (Information Technology Research in the Interest of Society o CITRIS) [21].

Figura 2.1: Mote MicaZ: tamaño(mm): 58x32x7 peso (gramos): 18 (Sin baterías)

Un nodo sensor está compuesto generalmente por una unidad de microcontrolador o unidad de procesamiento sencilla, una pequeña memoria, sensores, una fuente de alimentación eléctrica y un dispositivo de comunicación inalámbrico, que le permite comunicarse e intercambiar datos con otros motes [18, 19, 33].

Este tipo de dispositivos requieren de un sistema de operación específico para redes de sensores. En la actualidad, TinyOS es el sistema de operación más utilizado, posee una arquitectura basada en componentes que permite una rápida implementación mientas minimiza el tamaño del código. Las aplicaciones para los nodos son desarrolladas en un lenguaje llamado NesC, que es una extensión del lenguaje C diseñada para incorporar los conceptos y modelos de ejecución de TinyOS.

Idealmente, cada nodo sensor es capaz de sobrevivir con un par de baterías AA por lo menos un año [16]. Cada lectura que realiza y cada bit de datos que es transmitido consumen su batería y acercan al dispositivo a su fin operacional. Para evitar esto, los

nodos sensores deben seguir una ”dieta”muy estricta de consumo de potencia, funcionando en ciclos de bajo consumo. El nodo sensor es activado durante un porcentaje pequeño del tiempo para lecturas programadas o para recibir o transmitir datos de sus dispositivos vecinos [16], luego vuelve a un estado de ahorro de energía, en el que mantiene la mayoría de sus componentes apagados, consumiendo muy poca potencia.

Los nodos sensores pueden enviar alarmas, si las condiciones que se están monitorizando cambian de acuerdo a los parámetros que estaban programados [15]. Por ejemplo, las empresas en una cadena de suministros congelados, pueden usar redes de sensores en conjunto con etiquetas RFID (Radio-frequency identification) para monitorizar el cambio de condiciones durante la distribución de los productos [40], también pueden monitorear la correcta operación de equipos [31]. Las Redes de Sensores están siendo examinadas para su uso en aplicaciones de mantenimiento basado en condición [1, 26, 17], monitoreo ambiental [30, 6], agricultura [23], biología de la vida salvaje [27, 24], seguridad [49], en el ámbito militar [25, 46] e ingeniería estructural [51, 36].

2.1.2. Estación Base o SINK

Definición 2.3 (Estación Base o SINK)**.** Una estación base es un nodo encargado de recibir la información enviada por los demás nodos que conforman la red de sensores. Por lo general, tienen alimentación eléctrica y su configuración no es exactamente igual a los demás nodos. Es posible aprovechar su poder de procesamiento para hacer algunas transformaciones a los datos, antes de enviarlos al repositorio o servidor que se encargará de su procesamiento.

Por sus características, algunos diseñadores de protocolos le asignan a la estación

base funciones adicionales a las antes indicadas. Por ejemplo, en los protocolos basados en consultas debe enviar los parámetros de la consulta, también llamado ”interés”, así como del envío de sus posteriores actualizaciones [16]. Sirve como intermediario entre aplicaciones externas y la red de sensores, de manera que suele estar relacionado con las interfaces necesarias para tal fin. También es posible que tenga bajo su responsabilidad algunas tareas de administración de la red.

2.1.3. Gateways para RIS

En una implementación real, no es de utilidad una red de sensores que no intercambia información con otros dispositivos.

Definición 2.4 (Gateways para RIS)**.** Un gateway es un dispositivo que permitirá conectar la Red Inalámbrica de Sensores (RIS) a una red de mayor cobertura, como Internet por ejemplo.

Desde el exterior algunos usuarios podrán tener acceso a la información que está siendo recolectada por los sensores, y la posibilidad de interactuar con la red y sus componentes. A través de un gateway se pueden realizar incluso actividades de administración y gestión.

2.2. Protocolos de Encaminamiento: Restricciones y Retos

Un protocolo para redes de sensores debe permitir configurarse de tal forma que su operación no requiera de la atención de personal. A diferencia de las redes móviles

ad-hoc, las redes de sensores no tienen grandes requerimientos de movilidad. También se diferencian de otras redes inalámbricas, como por ejemplo WLAN, que fueron diseñadas para tener un mayor alcance y que por lo tanto requieren una fuente de energía constante. De allí que el diseño de protocolos para RIS considere características específicas que no son contempladas en otras tecnologías. Los criterios de diseño para una red de sensores dependen directamente de la aplicación ya que no es lo mismo la latencia para una aplicación de monitoreo, que para una aplicación de vigilancia.

El estándar IEEE 802.15.4 es utilizado prácticamente por todos los dispositivos sensores inalámbricos en la actualidad. Su especificación sólo incluye las capas a nivel físico y de enlace, por lo que las labores de la capa 3 (capa de red) deben ser implementadas de acuerdo a las necesidades de la aplicación. Dado que existe una estrecha relación y comunicación entre las capas, deben comprenderse sus estructuras al diseñar y desarrollar aplicaciones para redes de sensores. Por esta razón se ha agregado, en el apéndice A, una breve descripción del protocolo IEEE 802.15.4 y de su arquitectura.

Dado que no necesariamente puede establecerse un enlace directo entre un nodo cualquiera de la red y la estación base, se requiere una topología de red de múltiples saltos y de un algoritmo para determinar la ruta que seguirá el mensaje. Se trata de topologías dinámicas con nodos que pueden dejar de operar por fallos físicos o falta de baterías, con restricciones de ancho de banda, enlaces con capacidades variables y equipos que pueden operar con restricciones de energía. Todos estos factores traen como consecuencia frecuentes e impredecibles cambios en la topología que el protocolo de encaminamiento debe manejar.

Los retos a los que está expuesto un protocolo de encaminamiento para redes de sensores son: escalabilidad al incrementar la cantidad de nodos durante la operación,

tomar en cuenta el tiempo de transmisión y la potencia empleada, sin perder de vista la latencia que puede existir en la búsqueda de las rutas. También debe considerar la tasa de datos de las redes inalámbricas, convergencia rápida y la reacción eficiente a los cambios topológicos y demandas de tráfico.

2.3. Características de las Aplicaciones de Monitoreo que usan WSN

Con el desarrollo de tecnologías LR-WPAN (Low Rate - Wireless Personal Area Network) como es el caso de IEEE-802.15.4 se ha incrementado el desarrollo de distintos tipos de aplicaciones que son enumerados en el apéndice B.3. Sin embargo, este trabajo se enfoca principalmente en las aplicaciones de monitoreo y control las cuales poseen las siguientes características:

- Automatizar la obtención de los datos de nodos sensores remotos disminuyendo la intervención de usuarios.
- Configurar y ejecutar distintos sistemas desde un punto central.
- Proveer información detallada para mejorar el mantenimiento preventivo.

Las aplicaciones de recolección de datos del ambiente típicamente usan protocolos de encaminamiento basados en árbol: cada árbol tiene como raíz un nodo base con una mayor capacidad de recursos. Los nodos con mayor cantidad de descendientes transmiten más datos, así que pueden ser puntos de embotellamiento que pueden presentar

problemas de energía. Normalmente necesitan bajas tasas de datos y tiempo de vida extremamente largos.

Una vez la red es desplegada, los nodos deben descubrir la topología de la red y estimar una estrategia óptima de encaminamiento. Algunas implementaciones aprovechan que la topología física de red es relativamente constante para calcular la topología óptima de la red externamente y solo comunicarle a los nodos, la información de encaminamiento que deben seguir.

Los períodos típicos de envío de mensajes periódicos varían de 1 a 15 minutos y los parámetros que comunmente se miden son: temperatura, intensidad de luz y humedad, que son parámetros que no cambian rápidamente y tienen bajas tasas de medición. En general, los datos son recolectados para futuros análisis por lo que este tipo de aplicaciones no tienen restricciones estrictas de latencia.

Los nodos sensores estarán en un modo de ahorro de energía la mayor parte de su tiempo; sólo serán despertados al momento de enviar y recibir datos. Eventualmente, los nodos fallarán por falta de energía, y el proceso de reconfiguración generará un gasto extra de energía de los nodos restantes. Sin embargo, no es un evento que suceda muy frecuentemente.

Los principales necesidades de los sistemas de monitoreo de ambiente son: largo tiempo de vida, bajas tasas de datos y topologías estáticas.

2.4. Aspectos a Considerar por los Protocolos de Encaminamiento para Aplicaciones de Monitoreo

En el caso particular de las aplicaciones de monitoreo, son dos los aspectos más importantes que deben tomarse en cuenta: La confiabilidad en la entrega de los mensajes y la inmediatez en la entrega de las alarmas.

Para mantener enlaces que garanticen la confiabilidad de los mensajes creemos que deben considerarse tres aspectos principales: batería disponible, número de saltos y calidad de enlace.

Para ahorrar energía debemos agregar mensajes, gestionar la energía de los nodos, reducir la cantidad de saltos y que el protocolo tenga una mínima carga de mensajes de control. Incluir todas estas características sugiere que el protocolo a su vez sea autoconfigurable.

A diferencia de los mensajes periódicos, las alarmas requieren que los mensajes lleguen lo antes posible a la estación base, de allí que los criterios de agregación y ahorro de energía son secundarios, siendo el atraso en la entrega de las alarmas el aspecto más importante.

2.5. Soluciones Relacionadas con las Métricas de Interés

A continuación se describen algunas de las soluciones propuestas por los protocolos encontrados durante el estudio del estado del arte (algunos de ellos son estudiados en

el siguiente capítulo) relacionadas con los aspectos considerados relevantes para las aplicaciones de monitoreo:

- Confiabilidad en la entrega de mensajes: Dado que las decisiones de encaminamiento son a un salto, los protocolos toman la decisión en función de la información que el nodo posee de sus vecinos. Por tanto, escoger el próximo salto debería tener alguna garantía de que la ruta que se selecciona llegará a la estación base. Lo que ofrecen los protocolos en este sentido consiste en establecer previamente caminos confiables o enviar copias de un mismo mensaje por distintos caminos para aumentar la probabilidad de éxito. En ambos casos hay un costo adicional ya sea en mensajes de control, como en el primer caso, o en mensajes de datos como el segundo. Además, hay que tomar en cuenta que quizás el vecino a un salto ofrece un excelente enlace y dispone de mucha batería pero el vecino a dos saltos puede tener problemas con alguna de estas dos métricas.

- Calidad de Enlace: Luego de estudiar varios protocolos, se pudo encontrar que hay protocolos que al considerar la calidad del enlace como métrica utilizan el valor de LQI (Link Quality Indicator) incorporado en los chips de radio CC2420, que en la actualidad es el chip de radio que incorporan la mayoría de los dispositivos sensores. Sin embargo, de acuerdo al estudio realizado por [48], para que el LQI realmente pueda tener una correlación con la tasa de paquetes recibidos debe ser calculada como un promedio de los valores obtenidos dentro de una ventana de un tamaño específico. Otro dato disponible para medir la calidad del enlace es el RSSI (Received Signal Strength Indicator). Algunos autores no lo consideran confiable debido a la asimetría del transmisor de radio [48]. Estudios

recientes utilizando el nuevo chip de radio CC2420, indican que dicho problema ha sido solventado aunque su correlación con la tasa de entrega de paquetes dependerá de si el valor obtenido de RSSI está dentro de un umbral específico.

- Ahorro de Energía: Una de las estrategias que han sido usadas para ahorrar energía consiste en disminuir la cantidad de mensajes a transmitir. Una de las propuestas consiste en sólo enviar mensajes cuando los datos medidos estén dentro de un umbral específico. Dichos umbrales son enviados desde la estación base vía broadcast a todos los nodos sensores quienes aprovechando su capacidad de procesamiento determinarán cuando enviar o no la información. La principal desventaja de esta propuesta es que si los nodos no reciben el umbral o una eventual actualización podrían dejar de enviar los datos recolectados.

Como se puede observar hay ideas interesantes para cada uno de los aspectos de interés. Sin embargo, no se ha encontrado un protocolo que los correlacione en función de satisfacer las necesidades de las aplicaciones de monitoreo. Es por esto que se plantea la posibilidad de proponer un nuevo protocolo de encaminamiento para redes de sensores que ofrezca confiabilidad en la entrega de los mensajes, utilizando para ello métricas como: batería disponible (y estrategias para su ahorro), número de saltos y calidad del enlace, considerando además mejoras sobre la implementación de estas métricas con base a lo detectado durante el estudio. De forma indirecta también se contribuirá con el tiempo de vida, la cobertura y la tasa de muestreo efectiva. Una definición de estas métricas puede encontrarse en el apéndice B.4

Capítulo 3

Trabajos Relacionados

El problema de diseñar protocolos que encaminar mensajes en redes de sensores ha sido abordado por distintos trabajos, la mayoría preocupados por el ahorro de energía en la red.

La nueva solución que se propone en este trabajo, consiste en diseñar un protocolo de encaminamiento que considera varias métricas a la hora de seleccionar las rutas a Sink. En este nuevo enfoque, se han mejorado las técnicas con las que son tratadas cada una de las métricas de interés, si las comparamos con otras propuestas. A diferencia de otros protocolos, dichas métricas son correlacionadas para obtener mayor confiabilidad en la entrega de los mensajes mientras se ahorra energía.

Existen varias clasificaciones para los protocolos de encaminamiento. Sin embargo, la más utilizada es en base a la estructura de la red. Esta clasificación divide a los protocolos en planos y jerárquicos. En la sección 3.1 se describirán algunas propuestas de protocolos planos, mientras que en la sección 3.2 se presentarán detalles de algunos protocolos jerárquicos.

3.1. Protocolos Planos

En los protocolos planos por lo general todos los nodos cumplen el mismo rol y colaboran juntos en las tareas de medición. Por lo general, no es posible asignarle un identificador único a cada nodo, el encaminamiento no esta basado en quien envía los datos, utiliza los datos que se transmiten para tomar decisiones de encaminamiento. La estación base hace una consulta y espera por la respuesta de los nodos sensores.

A continuación algunos protocolos planos que fueron estudiados:

- Inundación [4]
- SPIN (Sensor Protocol for Information via Negotiation) [12]
- Fidelidad Adaptativa Geográfica [3]
- Directed Diffusion [14]

3.1.1. Inundación

Inundación [4] es uno de los algoritmos de encaminamiento más sencillos de implementar y consiste en inundar la red con un mensaje, para que llegue a todos los nodos. Esta estrategia se basa en que cada nodo envía el mensaje a todos sus nodos vecinos, para garantizar que llega al nodo donde esa información puede ser procesada, almacenada o consumida. Para evitar que los mensajes estén circulando indefinidamente, un nodo reenviará sólo los mensajes que no ha recibido previamente (requiere para ello la identificación única de los nodos y de los mensajes). También pueden incorporar una

expiración en tiempo o en número de saltos a los mensajes. Si bien es relativamente sencilla de implementar, lo cierto es que implica enviar muchos mensajes y consumirá más energía de los equipos que en las otras estrategias de encaminamiento, además de lidiar con los problemas de redundancia de mensajes y contención que fueron estudiados en [53].

3.1.2. Fidelidad Adaptativa Geográfica

Por su parte, los protocolos de Fidelidad Adaptativa Geográfica [3], plantean la posibilidad de tener dos sensores redundantes pero coordinados, de forma tal que sólo uno de los nodos redundantes está encendido en un instante de tiempo. Esta característica permite dos aspectos muy importantes: en primer término, incrementa el tiempo de vida de la red de sensores y por otra parte, el hecho de que las mediciones se realicen con dos equipos reduce la posibilidad de obtener lecturas sesgadas, debido al funcionamiento inadecuado de alguno de los nodos sensores. La idea es dividir el área en rectángulos tan pequeños que cualquier nodo de un rectángulo pueda comunicarse con cualquier otro nodo de un rectángulo adyacente. Dado que todos los nodos conocen su localización, fácilmente pueden construir sus rectángulos de equivalencia, determinar los nodos que están en su mismo rectángulo y colaborar entre sí para determinar los patrones para dormir y despertar de los nodos.

3.1.3. SPIN (Sensor Protocol for Information via Negotiation)

SPIN [12] es un protocolo basado en negociación que considera que opera más eficientemente y ahorra más energía si envía información que describa lo que el sensor

ha medido, en lugar de la información como tal. En aplicaciones donde los mensajes de datos son largos este criterio es particularmente útil.

Este protocolo sustituye el simple envío de datos de un protocolo de inundación por un proceso de tres pasos. Para tal fin, incorpora tres tipos de mensajes: ADV, REQ y DATA. Cuando un nodo sensor obtiene un nuevo dato, ya sea por mediciones locales o de otro nodo, informa el nombre del dato a sus vecinos a través de un mensaje ADV. El receptor del dato puede comparar el nombre recibido con sus datos locales y si es desconocido lo puede solicitar enviando un mensaje de tipo REQ (si es un dato que ya ha recibido, simplemente lo ignora). Solamente cuando se recibe una solicitud es que se trasmite la información (mensaje de tipo DATA).

3.1.4. Directed Diffusion

Al igual que SPIN, Directed Diffusion es un protocolo centrado en los datos (en el apéndice B.3.5 se da una pequeña descripción de lo que esto significa) en donde, un nodo Sink envía a través de la red un mensaje - llamado mensaje de interés - especificando un conjunto de atributos que describen los datos deseados. Los nodos sensores que pueden producir datos unicamente envían información si han recibido algún interés que coincide con sus datos, a estos nodos se les llama nodos fuente. Un nodo intermedio almacena el interés, conjuntamente con los posibles vecinos más cercanos a Sink en un buffer. Cuando recibe datos que coinciden con el interés almacenado, selecciona del buffer el vecino al que reenviará el mensaje. [14]

Tanto los intereses como los mensajes de datos son representados como un conjunto de atributos valor - operación. El conjunto de atributos está predefinido y son bien

conocidos los tipos de datos de los atributos.

Dado que Directed Diffusion representa tanto la descripción de los datos (colocando nombres a los datos y especificando las interfaces que los proporcionan) así como la implementación concreta del encaminamiento, es posible encontrar distintos algoritmos de encaminamiento basados en la arquitectura de Directed Diffusion. A continuación se enumeran los algoritmos más conocidos: [13]

- Two-phase-pull: Como su nombre lo indica, su operación está compuesta por dos fases, en una primera fase se inunda la red con los mensajes de interés y luego se envía mensajes adicionales para fortalecer los caminos de los cuales se obtiene información. Se le llama pull debido a que es Sink quien inicia el proceso al enviar el interés con lo que intenta traer los datos de los sensores.

- One-phase-pull: Es similar al anterior, solo que este algoritmo elimina una de las fases de inundación de two-phase pull. Esto es posible sólo si se utiliza algún identificador de flujo para los mensajes de interés y existe una fuerte simetría en los enlaces. Los mensajes de interés aún inundan la red, formando relaciones directas padre-hijo entre el nodo que recibe por primera vez el mensaje de interés y el nodo que se lo ha enviado.

- push-diffusion: Este algoritmo es especialmente útil cuando se trata de una aplicación donde hay muy pocos generadores de información y muchos receptores. En este caso se invierten los roles definidos en los dos algoritmos explicados anteriormente. En lugar de que los Sink inicien el proceso al transmitir los intereses, son los nodos sensores los que envían datos exploratorios inundando la red (ya que aún no están configurados los caminos en los nodos intermedios). Una vez

que los datos llegan a Sink, son enviados mensajes que fortalecen los caminos que llevan la información del nodo sensor a Sink.

3.2. Protocolos Jerárquicos

En los protocolos jerárquicos, a un subconjunto de los nodos se le asignan tareas especiales de coordinación para contribuir en la escalabilidad, tiempo de vida y eficiencia en el consumo de energía. Un nodo coordinador puede ejecutar tareas de agregación de datos que recibe de los nodos sensores que tiene asignados para disminuir el número de transmisiones hacia la estación base.

A continuación algunos protocolos jerárquicos que fueron estudiados:

- LEACH (Low Energy Adaptive Clustering Hierarchy) [12]
- TEEN (Threshold-Sensitive Energy Efficient Protocols) [28]
- SAR (Sequential Assigment Routing) [4]
- DIRq [10]

3.2.1. LEACH

LEACH (Low Energy Adaptive Clustering Hierarchy) [12] es un protocolo jerárquico conformado por clusters. La formación de estos clusters es distribuida, basada en un subconjunto predeterminado de los nodos que se eligen aleatoriamente como Clusters Head. La función de este rol consiste en comprimir la información que recibe de los

nodos que conforman el cluster y enviar un sólo mensaje con la información agregada a la estación base reduciendo de esta forma la cantidad de transmisiones.

Se utiliza un esquema TDMA/CDMA MAC para evitar las colisiones entre los cluster e incluso intra-cluster. Este esquema no tiene que ver con la frecuencia de la adquisición de datos. Luego de un tiempo determinado se realiza la rotación del rol CH con la finalidad que sea equilibrado el gasto de energía realizando esta labor, se utiliza un algoritmo que busca que todos los nodos pasen por este rol.

3.2.2. TEEN

TEEN (Threshold-Sensitive Energy Efficient Protocols) [28] es un protocolo jerárquico conformado por clusters propuesto para aplicaciones de tiempo crítico.

El proceso de adquisición de los datos es constante en los nodos, aunque las transmisiones no son tan frecuentes. Un Cluster Head, envía a sus miembros un umbral fuerte, el cual indica el rango de valores que interesa del atributo que se mide y un umbral débil que indica la magnitud del cambio en el valor del atributo medido, que es representativo y que le indica al nodo que debe encender su transmisor y transmitir. El primero trata de disminuir el número de transmisiones permitiendo que el nodo transmita sólo cuando el atributo medido está en el rango de interés. Mientras que el débil por su parte, reduce aún más el número de transmisiones al evitar realizarlas cuando hay un cambio pequeño o no hay cambio en el valor medido. Asignar un valor pequeño para el umbral débil nos proporcionará unos valores más exactos de lo que está midiendo la red, con un costo mayor de energía. Cuando se realiza la rotación en el rol CH, son enviados los nuevos valores de los parámetros vía difusión.

La principal desventaja de este esquema es que si los nodos no reciben los umbrales, no enviarán información y el usuario no recibirá datos de la red a pesar que los nodos miden su ambiente continuamente.

En los casos en que la transmisión de un mensaje consume más energía que el proceso de adquisición, este esquema consume menos energía que las redes que establecen las rutas de antemano (protocolos proactivos).

Aunque este protocolo y el anterior poseen varias características en común: son jerárquicos, basados en clusters, con estaciones bases fijas, con criterios de agregación de datos, escalables, no están basados en consultas y no usan esquemas de negociación; se diferencian en la forma en que disminuyen la transmisión de datos. LEACH propone que el nodo coordinador reuna la información de varios mensajes en uno, mientras que TEEN propone el manejo de umbrales para determinar cuando debe realizarse el envío de información por parte de los nodos sensores.

3.2.3. SAR

SAR (Sequential Assigment Routing) [4] es un protocolo que ofrece la noción de QoS (Quality of Service) como criterio de encaminamiento. Sus criterios son los recursos de energía y QoS en cada camino y nivel de prioridad del paquete. El protocolo crea múltiples caminos desde el origen siendo este nodo la raíz del árbol que se forma. Al final cada nodo formará parte de un árbol. Al determinar la ruta se calcula una relación entre la prioridad del paquete y la QoS del camino para escoger cual utilizar. El protocolo debe periódicamente recalcular los caminos para estar preparado en caso de falla de alguno de los nodos.

3.2.4. DIRq

DIRq [10] es un protocolo basado en consultas inspirado en el protocolo SRT (Semantic Routing Trees) que disminuye el consumo de energía reduciendo la cantidad de mensajes a enviar. Si un nodo sensor ha registrado un valor V_1 para un parámetro deseado y para el siguiente período de medición obtiene el mismo valor o uno similar, en un intervalo entre $(V_1 - x, V_1 + x)$ entonces no debe enviar nada a la estación base. Si la estación base no recibe ningún mensaje de un nodo específico entonces asume que este nodo ha medido un valor que no ha cambiado mucho con respecto a lo que ha reportado recientemente. Para permitir una entrega precisa de las solicitudes, todos los nodos de la red deben tener una capacidad de almacenamiento de información, lo cual también puede ser considerado una desventaja, dependiendo de la cantidad de información almacenada, de la topología y del número de nodos. DirQ es un protocolo adecuado para situaciones donde el número de solicitudes es alto y los momentos de envío de las solicitudes es conocido.

Capítulo 4

Solución Propuesta

En este capítulo se describe la solución propuesta en este trabajo, que consiste en el diseño de un nuevo protocolo de encaminamiento para redes de sensores, que se llama *SHRP* (siglas de *Simple Hybrid Routing Protocol*) que es proactivo, jerárquico y que toma en cuenta varias métricas a la hora de escoger el encaminamiento de los mensajes.

En la sección 4.1 se describe la arquitectura del protocolo, luego en 4.2, se presentan las funciones que los nodos pueden desempeñar dentro del protocolo. En 4.3 se describe la configuración de la topología. Posteriormente, en 4.4 se detallan los mensajes que forman parte del protocolo, en 4.5 se explican las métricas utilizadas y finalmente en 4.6 se presenta los criterios para seleccionar los caminos.

4.1. Arquitectura

SHRP es un protocolo que establece y mantiene, de forma proactiva, una topología que ofrece confiabilidad en la entrega de los datos que son enviados a la estación base.

Para lograrlo utiliza métricas como la batería local disponible, número de saltos hasta sink y la calidad del enlace entre los nodos vecinos para escoger la mejor ruta.

Periódicamente se están monitoreando estas métricas y se eliminan de la tabla de encaminamiento, aquellos nodos vecinos que no contribuyen al mantenimiento de una topología conectada de forma confiable:

- La calidad del enlace se ve afectada por fenómenos de propagación e interferencias. Todos estos problemas son reflejados en las métricas LQI y RSSI. Periódicamente cada nodo eliminará a aquellos vecinos que presentan un enlace por debajo de los umbrales mínimos previamente establecidos. En algunos casos, los problemas relacionados con la calidad del enlace son temporales. El protocolo agregará nuevamente los vecinos, una vez que la calidad del enlace mejore.
- Dado que la energía del nodo es proporcionada por baterías, con el transcurrir de su operación, el nodo consumirá su batería disponible. Periódicamente, cada nodo debe validar que posee suficiente energía disponible para ejecutar, lo que llamamos, un ciclo de trabajo mínimo (ver ecuación 4.1), eliminándose de las tablas de encaminamiento al poseer menos de dicha cantidad.

  Ecuación 4.1: Ciclo de Trabajo Mínimo

  $$MinimumTaskCycle = CCA + Sensing + Transmission + Reception + IdlePeriod$$

  Un ciclo de trabajo mínimo es la suma de la energía necesaria para acceder al medio (CCA), obtener el dato a través del sensor, transmitir el valor obtenido, recibir mensajes de los vecinos y finalmente el tiempo que se consume mientras duerme.

La operación del protocolo se puede clasificar en tres etapas: descubrimiento, operación y mantenimiento. En la fase de descubrimiento se establecen los vecinos y rutas para cada nodo. En la fase de operación se encaminan los distintos mensajes de datos y periódicamente se lleva a cabo una fase de mantenimiento de la topología que permite detectar posibles problemas en la red, ya sea en los enlaces o en los nodos.

De acuerdo a la funcionalidad del nodo, existe una estructura jerárquica dentro de la red en *SHRP*. Por una parte están los nodos coordinadores que se encargan del encaminamiento, a estos nodos se asocian los nodos sensores que sólo llevan a cabo las tareas de sensado.

Decimos que es un protocolo híbrido porque a diferencia de los protocolos estudiados y brevemente comentados en el capítulo 3 . *SHRP* considera varias métricas a la hora de seleccionar el mejor camino a Sink.

Dado que la transmisión es la actividad que más energía gasta en las redes de sensores [38], los nodos coordinadores pueden agregar varios mensajes de datos y enviarlos en un solo paquete.

Para incrementar aún más el ahorro de energía se sugiere que la aplicación de monitoreo también implemente políticas para el ahorro de energía. Para las aplicaciones que realizan mediciones periódicas, se sugiere que con el objetivo de ahorrar energía, no todos los mensajes periódicos sean enviados a la estación base. Cada nodo sólo envía datos que han cambiado con respecto a la última medición. Y para descartar posibles problemas de pérdida de paquetes, la aplicación puede establecer que cada cierto tiempo se envíen los datos de forma obligatoria.

4.2. Funciones de los Nodos

Existen cuatro tipos de nodos en *SHRP*: Los nodos sensores, nodos coordinadores (primarios y secundarios) y el nodo Sink.

4.2.1. Nodo Sensor (SN)

Este es un nodo que usa uno o más sensores para recolectar periódicamente una medida de un sistema físico y que tiene que enviar a su nodo coordinador. Entre cada período de recolección de datos el nodo sensor puede dormir.

4.2.2. Nodo Coordinador (CN)

Este nodo tendrá dos funciones principales: (i) Encaminar los mensajes de datos que vienen tanto de los nodos sensores así como los que provienen de otros nodos coordinadores; (ii) Agregar mensajes antes de enviar los mensajes recibidos, para de esta forma disminuir el número de transmisiones. Algunos nodos CN podrán ser configurados como nodos coordinadores secundarios (CNsec) y serán instalados muy cercanos a los primarios (CNpr), dichos nodos secundarios sólo comenzarán a trabajar si el nodo primario deja de funcionar.

4.2.3. Nodo Sink

Es el nodo a donde debe llegar la información obtenida por los demás nodos sensores. Para poder intercambiar información de monitoreo, este nodo debe ser o estar

conectado a un gateway que le permita comunicarse con sistemas externos.

4.3. Configuración de la Topología

SHRP fue desarrollado para redes de sensores que no requieren movilidad. La topología de la red puede ser definida a través de un estudio realizado en el sitio, de forma tal que cada nodo *SN* tenga conexión física con, al menos, un nodo *CN*. Se utilizará un protocolo de autoconfiguración para establecer la asociación entre *SN* y *CN*. Cada *CN* puede tener uno o más vecinos, algunos de ellos tendrán alcance al nodo Sink directamente. Cada mensaje enviado llegará a Sink a través de los nodos *CN* que formen parte de la mejor ruta definida por el protocolo *SHRP*. En las figuras 4.5 y 4.6 se pueden apreciar ejemplos de estas topologías.

Durante el despliegue de la red, algunas políticas pueden ser consideradas para garantizar la redundancia de los componentes de la red. Incluso, diferentes nodos pueden estar conectados a los mismos sensores (en los casos en que los sensores son costosos o difíciles de adquirir). Si es posible agregar nodos adicionales, que proveean rutas redundantes, se impactará positivamente la topología de la red, incrementando su tiempo de vida. Esto es factible dado el bajo costo de los nodos sensores (un kit de desarrollo con 10 nodos sensores cuesta alrededor de 780 dolares).

Los nodos coordinadores redundantes, que estén cercanos a otros motes pueden ser usados como nodos secundarios (CNsec). Cada CNsec estará en modo Sleep y periódicamente verificará que su nodo primario CN esté funcionando. Si no recibe una respuesta durante cierto tiempo, asumirá que su nodo primario ha desaparecido convirtiéndose en nodo primario.

4.4. Mensajes SHRP

Existen dos tipos de mensajes en *SHRP*: los mensajes de control y los mensajes de datos.

Los mensajes de control son usados para definir y mantener las rutas de *SHRP*. NMI, Hello y las alarmas son mensajes de control que son explicados en detalle en 4.4.2, 4.4.3 y 4.4.4. Por su parte, los mensajes de datos transmiten información de monitoreo recolectada por los nodos sensores y serán detallados en 4.4.5

Todos los mensajes de *SHRP* utilizan un mismo formato de mensajes, lo cual proporciona escalabilidad y uniformidad en su manejo. Dicho formato esta compuesto de un encabezado y un cuerpo o carga útil.

El Encabezado proporciona información sobre el tipo y composición del contenido que se encontrará en la carga útil, lo cual permite establecer estrategias sin tener que revisar siquiera el contenido del mensaje.

La carga útil es de tamaño y composición variable dependiendo del tipo de mensaje que se desea transmitir, el cual es indicado en el encabezado. En lo sucesivo cuando se detalle la composición de los mensajes de *SHRP* nos referimos a la información que viene en la carga útil del mensaje.

4.4.1. Encabezado SHRP

En la figura 4.1 se presenta el formato del encabezado de todos los mensajes de *SHRP*.

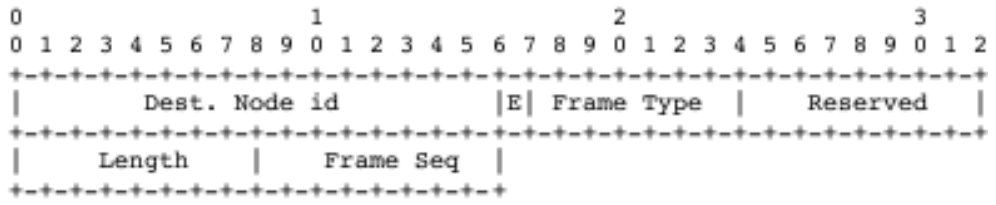

Figura 4.1: Formato del Encabezado de los Mensajes

El encabezado esta compuesto por los siguientes atributos:

- **id Nodo Destino** Identificación del nodo destino. Cada nodo tiene desde su configuración un ID único.
- **Marco extendido** tiene el valor uno (1) si el paquete tiene más de un mensaje, cero (0) en caso contrario.
- **Tipo de Marco** Para los paquetes que contienen un sólo mensaje este campo indica el tipo de mensaje que se envía. Cuando dos o más mensajes son transmitidos, este campo indica el tipo del próximo mensaje.
- **Longitud del Marco** Tamaño en bytes del paquete.
- **Id secuencia del Marco** Este campo es incrementado en uno cada vez que un nuevo paquete es transmitido.

4.4.2. Mensaje de Informacion de la Red (NMI)

El propósito de este mensaje (NMI, por sus siglas en inglés) es proveer información local de los vecinos que rodean a cada uno de los nodos de la red. Con esta información es posible definir la topología de la red y construir la tabla de vecinos para cada uno de los nodos. Todas las métricas incluidas en el mensaje NMI son actualizadas con los datos del nodo receptor, recalculando sus valores para luego retransmitirlos a sus vecinos.

El formato del mensaje NMI se muestra en la figura 4.2.

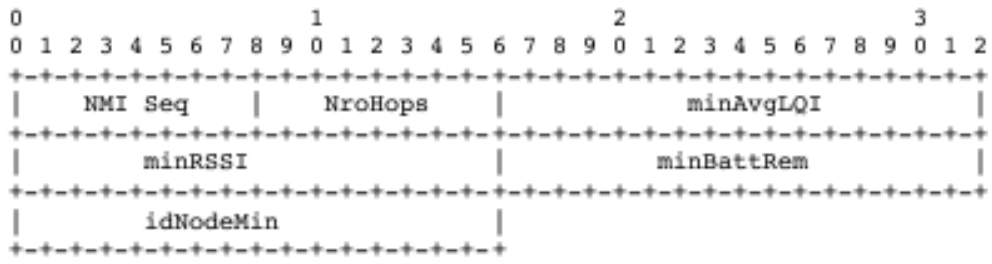

Figura 4.2: Formato del mensaje NMI

El nodo Sink debe enviar un mensaje NMI periódicamente cada NMI_INTERVAL. NMI es un mensaje enviado por difusión. Con la información recibida en cada mensaje, los nodos deben recalcular todas las métricas y actualizar la información sobre los vecinos a un salto. El número de secuencia en el mensaje refleja la frescura del mensaje y evita el procesamiento redundante.

Con un nuevo número de secuencia, el nodo debe reiniciar sus cálculos de la mejor ruta. El nodo debe enviar un mensaje NMI cada vez que consiga un mejor camino para alcanzar a Sink. Por su parte los nodos receptores, deben verificar si el nodo que envía

es un buen vecino. De esta forma, se mantiene actualizada la topología de la red ante cambios inesperados. De este mensaje también se obtiene la calidad del enlace entre el nodo que recibe y el que envía.

Antes de enviar su mensaje NMI, el CN hace una autoevaluación de su batería disponible. Si este valor está por debajo de un umbral establecido, no enviará el mensaje a sus vecinos ya que no se considera un buen vecino para el cálculo de la mejor ruta. De esta forma, cada CN sólo tendrá vecinos con la batería suficiente para encaminar los mensajes de datos.

Si un nodo decide no enviar su mensaje NMI, debe enviar un mensaje especial de alerta llamado *Control Alarm Message (CAM)* al nodo Sink, para informar que el nodo dejará las listas de vecinos pronto. La principal idea es evitar la pérdida de conectividad de la red.

Antes de actualizar las tablas de encaminamiento, el nodo debe verificar que exista un buen enlace con el vecino. Las métricas relacionadas con la calidad del enlace (RSSI y LQI) deben estar por encima de los umbrales mínimos establecidos para cada uno de ellas minRSSI y minLQI respectivamente. El algoritmo 1 muestra el procedimiento para verificar a un vecino:

Algoritmo 1 Verificación de Vecinos

```
if vecino(RSSI) < minRSSI then
   Descartar al nodo como vecino
else
   if vecino(LQI) < minLQI then
      Descartar al nodo como vecino
   end if
end if
marcar al nodo como buen vecino
```

De forma intuitiva podemos decir que un nodo vecino es un nodo CN que tiene suficiente batería para garantizar la entrega de mensajes y ofrece un enlace confiable en términos de señal de radio, para alcanzar directamente o a través de otros nodos confiables al nodo Sink.

4.4.3. Mensaje Hello

Para lograr establecer la topología de la red, es necesario que el mensaje NMI enviado por Sink recorra toda la red. El tiempo de convergencia y la cantidad de mensajes involucrados deben ser tales que permitan que la información llegue hasta el nodo más alejado de la red, pasando por tantos saltos como sean necesarios.

Se puede pensar que este proceso no debe ser muy frecuente debido a los costos de tiempo/energía asociados. Sin embargo, los cambios en la topología causados por problemas de batería, interferencias, etc, pueden aparecer en cualquier momento.

Una vez que NMI ha definido la topología de la red, se utilizan mensajes Hello para detectar cambios en la red. Este mensaje es menos costoso, en términos de sobrecarga, que NMI porque cada nodo envía periódicamente sólo un mensaje Hello a sus vecinos.

El formato del mensaje Hello se detalla en la figura 4.3.

Cada CN debe enviar un mensaje Hello periódicamente cada HELLO_INTERVAL o cuando detecte que ha cambiado de rango de batería de acuerdo a su energía disponible. Más adelante, en la sección 4.6.2 se explica la conformación y cálculo de los rangos de batería. Cuando un nodo recibe un mensaje Hello, actualiza las métricas de su vecino y verifica que utiliza la mejor ruta entre las opciones disponibles.

Figura 4.3: Formato del mensaje Hello

CN espera un cierto tiempo para recibir el próximo mensaje Hello de sus vecinos.

- Si un nodo C no recibe el mensaje Hello de un nodo B, previamente definido como su vecino, debe verificar si el nodo B es parte de la mejor ruta a Sink y si existe una ruta alterna, en este caso, CN cambia su mejor ruta. En el ejemplo de la figura 4.4(a), supongamos que el nodo A es Sink, el nodo C tiene dos opciones de encaminamiento: La mejor ruta es $C - B - A$, si el enlace $C - B$ tiene problemas se reconfigura con $C - D - A$

- Si el nodo solamente disponía de una ruta, debe enviar un mensaje de alarma, llamado *Orphan Node*, dirigido al nodo Sink para que éste a su vez, inicie el proceso de redescubrir la topología de la red enviando un nuevo mensaje NMI, con lo que reconfigurará toda la red. En la figura 4.4(b) se muestra la topología que descubrió el protocolo. En este caso el nodo C tiene sólo una opción para enviar sus mensajes, $C - B - A$, aunque el nodo C tiene alcance con el nodo D, si el enlace $C - B$ tiene problemas se envía una alarma para redescubrir la topología.

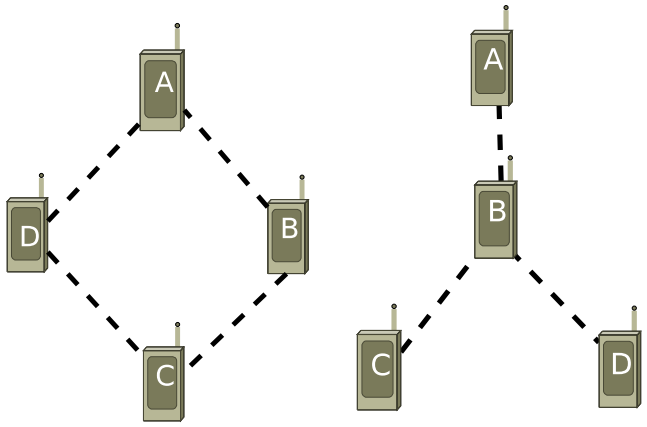

Figura 4.4: Ejemplos de topologías para ilustrar las estrategias en el manejo del mensaje Hello

4.4.4. Alarmas

Los mensajes de alarma permiten informar a Sink sobre cambios que pueden afectar la topología de la red y que permitirán tomar acciones preventivas específicas para mantener la conectividad.

El nodo que genera la alarma difunde el mensaje en la red, aumentando la probabilidad de que el mensaje sea recibido por sink al ser procesado por todos los nodos que lo reciban.

Los receptores escogerán un vecino de la tabla generada por *SHRP* considerando únicamente mínima cantidad de saltos y obviando criterios como rangos de baterías o agregación, ya que en el caso de las alarmas se busca que la información llegue lo antes posible, aunque esto involucre un mayor consumo de energía.

En 4.4.2 y 4.4.3 se han mencionado casos donde el protocolo dispara alarmas como parte de su funcionamiento.

4.4.5. Mensajes de Datos

Se definen tres tipos de mensajes de datos: (i) periódicos; (ii) alertas; (iii) alarmas [9].

La estación base envía un mensaje de consulta con la información que el sistema de monitoreo está interesado en recolectar periódicamente. Basado en este mensaje, los nodos sensores saben cuando tienen que medir y cuando deben enviar los datos recolectados.

Los mensajes de alerta, por su parte, son enviados cuando los valores de los parámetros medidos están sobre el valor promedio esperado, el cual es especificado por el sistema de monitoreo [7].

Los mensajes de alarma son enviados cuando los datos medidos están por debajo del mínimo o por encima del máximo, estos valores también son especificados por el sistema [7]. Estos mensajes son enviados de la misma forma en que se envían las alarmas de control, explicadas en la sección 4.4.4

4.5. Métricas usadas por SHRP

SHRP utiliza las siguientes métricas: Batería disponible, calidad de enlace y número de saltos para seleccionar la mejor ruta a Sink

4.5.1. Batería Disponible

Cada nodo evaluará su batería disponible y la incluirá en las métricas que transmitirá a sus vecinos. Al decidir sobre cual es la mejor ruta, el nodo preferirá aquellos caminos que ofrezcan mejores garantías, en cuanto a la energía que tienen disponible. Por otra parte, tal como se detalló en 4.1, se excluirán de la tabla de encaminamiento aquellos nodos que no tengan suficiente batería disponible para operar.

4.5.2. Número de saltos

Esta métrica indica la cantidad de nodos por la que debe pasar un mensaje para llegar al nodo Sink. Es calculada por el mensaje NMI que recorre toda la red. Reducir la cantidad de saltos es una política para ahorrar energía, basado en lo costoso que es la transmisión de los datos en términos de gasto de energía. Por otra parte, su disminución colabora en la reducción del retardo en la entrega.

4.5.3. Calidad de Enlace

El estándar IEEE-802.15.4 ofrece mecanismos para evaluar la calidad del enlace a nivel de la señal de radio. En particular, el chip de radio CC2420 basado en dicho estándar es actualmente el más utilizado en la investigación y desarrollo de redes de sensores.

CC2420 opera en la banda 2.4 GHz ISM con un tasa de ancho de banda efectiva de 256 kbps, tiene 16 canales y cada canal ocupa 3 MHz. CC2420 utiliza un esquema de codificación en el que utiliza 32 chips para codificar un simbolo de 4 bits. Una vez los datos estan codificados utiliza la modulación OQPSK (siglas de Offset quadrature

phase shift keying) para transmitirlos [50]. CC2420 ofrece dos métricas muy utiles RSSI (Received Signal Strength Indicator) y LQI (Link Quality Indicator).

- RSSI es un indicador de la fuerza de la señal que puede ser utilizado como una manera simple de determinar si existe una buena tasa de recepción de paquetes PRR (por sus siglas en inglés Packet Reception Rate). Si el RSSI está por debajo del umbral definido en [48], -87 dBm, no se puede garantizar que exista un enlace confiable. A pesar de que es una métrica que se obtiene de los paquetes recibidos, puede ser usada como una métrica para la transmisión de paquetes, dado que los nuevos chips de radios como el CC2420 tienen un comportamiento simétrico con respecto a la calidad de enlace [48].
- LQI es un parámetro definido por el estándar IEEE-802.15.4 y que es implementado en los dispositivos de radio CC2420. Este representa la tasa de error en los chips transmitidos, calculados al correlacionar los primeros ocho símbolos, después del SFD (Start Frame Delimiter) de cada paquete [50]. Estudios como los realizados por [48] indican que el valor de LQI puede variar de forma repentina y que su uso puede generar cambios que afectan las decisiones del protocolo. Para obtener una buena correlación entre el LQI y el PRR debe calcularse un promedio de los LQI, denominado *AvgLQI*, usando para ello los datos recibidos dentro de una ventana de tamaño determinado.

Dado que RSSI tiene una zona donde no garantiza su correlación con PRR [48] se decidió utilizarla conjuntamente con el promedio de LQI al momento de evaluar los enlaces.

Las métricas LQI y RSSI son tomadas de la capa física de la red inalámbrica, siendo

valores que pueden obtenerse de todos los mensajes recibidos, tanto de control como de datos. En nuestros experimentos estamos usando el chip de radio CC2420 [50].

4.5.4. Cálculo de las métricas

Dado que la decisión de encaminamiento es a un salto, se puede pensar que la información disponible es local y de hecho, muchos protocolos funcionan de esta manera. Sin embargo, en el caso de *SHRP*, las métricas son calculadas con el criterio que llamamos Min-Max. Esto significa que las métricas de un vecino que forma parte de una ruta a la estación base no sólo representan la información de dicho nodo, sino que contempla la información del peor enlace (Min) que hay entre él y la estación base, sin tener que almacenar cada uno de los datos de los nodos intermedios, que por demás no es factible debido a las restricciones de almacenamiento del nodo. Luego, entre las posibles rutas se escogerá aquella que ofrezca mejores valores (Max).

Sea mt_i el valor de la métrica m transmitida por el vecino i, sea V el conjunto de los vecinos del nodo y sea mf el valor de la métrica m obtenida por el nodo directamente de la capa física, el valor a transmitir por el nodo es:

$$mt = Min(Max_{v \in V}(mt_v), mf)$$

Estos valores Min-Max son los que se almacenan en las tablas de encaminamiento y que se utilizan cuando los nodos intercambian información. De esta forma se realiza el cálculo de las métricas: batería remanente, RSSI y AvgLQI.

4.5.5. Umbrales Utilizados

Algunos trabajos han sido realizados para determinar los valores mínimos razonables para ser usados como umbrales con los que se comparan las métricas usadas por *SHRP*. En el caso de la batería disponible, fue realizado un estudio en [37] del consumo de batería usando dispositivos CC2420 para determinar el valor de BattMin que una batería debe tener para poder transmitir un mensaje. Este puede ser usado para establecer algunas comparaciones, en términos de consumo de energía. En [48] se muestra una correlación entre el promedio LQI y la tasa de recepción de paquetes PRR. Esta información puede ser usada para seleccionar un valor mínimo de operación, que de acuerdo a la tasa de recepción de paquetes de la aplicación garantice la la entrega del paquete al próximo nodo.

4.6. Selección del camino

Cada nodo hace la selección del próximo salto que le permita al mensaje alcanzar a Sink, basado en la información local de sus tablas de encaminamiento. Al seleccionar la mejor ruta, el nodo preferirá aquella que proporciona mayor confiabilidad, es decir, la ruta que garantiza mayor energía disponible y calidad de enlace a lo largo del camino hasta la estación base. En algunos casos esto puede requerir mayor cantidad de saltos.

4.6.1. Información de los vecinos

El nodo mantiene los datos de cada vecino en la siguiente tupla:

$$\{id, Nrosaltos, MinBattRem, idNodeMin, AvgLQI, RSSI\}$$

- **id** Identificación del nodo.
- **Nro saltos** Cantidad de nodos intermedios por los que debe pasar un mensaje antes de alcanzar a la estación base.
- **MinBattRem** Menor valor de bateria disponible entre los nodos que forman el camino hasta la estacion base
- **idNodeMin** Identificación del nodo cuya bateria disponible es MinBattRem
- **AvgLQI** Promedio de la métrica LQI del nodo calculada dentro de una ventana de mensajes recibidos específicada por el protocolo
- **RSSI** Valor actual del RSSI para el enlace con el nodo vecino

Esta información es mantenida a través de los mensajes NMI y Hello discutidos en 4.4.2 y 4.4.3 respectivamente. En los ejemplos que se presentan es esta sección omitiremos los valores de la calidad de enlace para concentrarnos en los criterios de batería y cantidad de saltos ya que, como se explicó en 4.1, sólo permanecen como vecinos aquellos nodos con los que se tiene un buen enlace y que además no tienen problemas de batería.

Al evaluar los distintos caminos, se utilizarán las métricas de batería disponible y número de saltos. Dentro de la información de NMI que envía el vecino se conoce: cuál es la menor batería disponible en el camino, cuál es el nodo que dentro del camino

posee dicho valor mínimo y la cantidad de saltos requeridos para llegar a Sink. Usando en conjunto ambas métricas es posible obtener los distintos caminos, sin ciclos, que llegan a Sink indicando cuál es la batería mínima disponible en cada caso.

Esta política elimina los ciclos, ya que al ser una topología de árbol que se conforma a partir de un mensaje enviado desde la raíz, todo ciclo será descartado como camino válido al existir un camino válido previamente incluido con el mismo nodo con batería mínima y menor cantidad de saltos.

En el siguiente ejemplo podemos ver la conformación de una topología:

Ejemplo 4.1. En la figura 4.5 las líneas punteadas representan las relaciones de vecindad luego de establecerse la topología. Si representamos a los vecinos del nodo B utilizando la tupla explicada previamente, obtenemos:

$$V_B = ((A, 3, 5, A), (E, 4, 5, E))$$

A diferencia de los protocolos basados en cantidad de saltos, en este caso se puede apreciar como el nodo B mantiene al nodo E como vecino a pesar que está a un salto más que el camino que ofrece el nodo A. Esto se debe a que corresponden a dos caminos válidos que no producen ciclos. La primera tupla nos indica que el camino a sink es a través del nodo A realizando tres saltos y que además es el mismo nodo A el que posee la menor batería disponible entre los nodos por los que pasará el mensaje antes de llegar a Sink. Por su parte, la segunda tupla presenta un camino a través del nodo E realizando cuatro saltos, siendo E el nodo con menor bateria en dicho camino. Al mantener la información de cuál es el nodo de batería mínima, es posible diferenciar

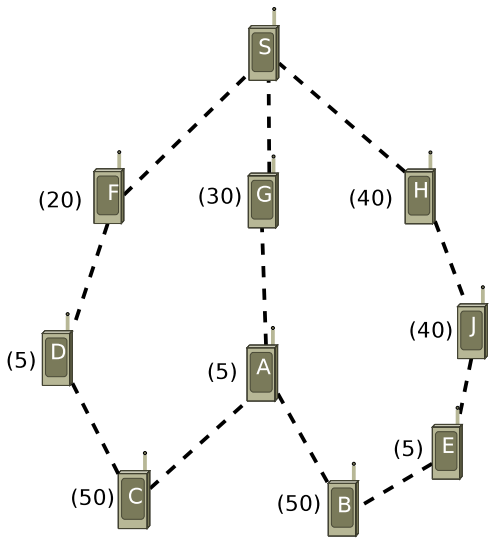

Figura 4.5: Ejemplo de una conformación de topología, se indican los valores de batería disponibles en cada nodo

los caminos. Con esta política se busca obtener la mayor cantidad de caminos válidos posibles.

Veamos otro ejemplo que ilustra como un nodo puede tener vecinos a distinta cantidad de saltos.

{id, Nro saltos, MinBattRem, idNodeMin, AvgLQI, RSSI}

Ejemplo 4.2. Estudiemos los vecinos del nodo K en la figura 4.6. Los nodos A, B, E, G, H, J y Sink no tiene alcance con K; esto puede ser motivado a problemas de obstáculos, distancia o interferencias que no le permiten tener alcance directo.

La tabla de vecinos del nodo K es:

$$V_K = (F, 1, 10, F), (D, 2, 10, G), (C, 3, 10, H), (L, 4, 20, J)$$

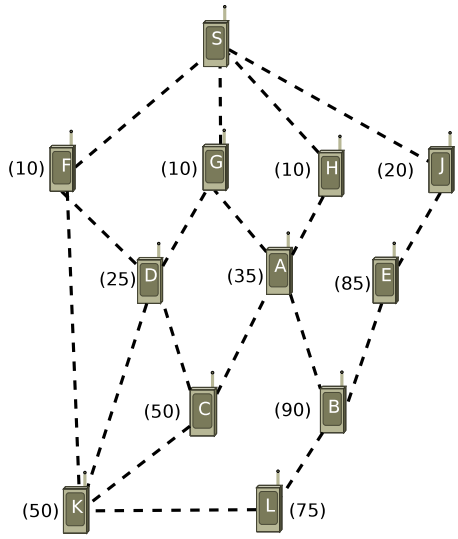

Figura 4.6: Múltiples caminos válidos para alcanzar Sink desde un nodo K, con distintos números de saltos

Aunque el nodo K también podría recibir del nodo D un NMI con los siguientes valores: $(D, 2, 10, F)$, en ese caso el mensaje sería descartado, ya que el nodo K ha recibido del nodo F un NMI con el mismo nodo con batería mínima y con menor número de saltos. De forma similar sucede con algunos mensajes recibidos de los nodos C y L. Si el camino seleccionado por K pasa por el nodo D, el NMI que envía a los demás nodos es recibido por el nodo D ya que está dentro del alcance del nodo. Sin embargo, dicho nodo lo descartará ya que el nodo mínimo es el mismo, eliminando a su vez la posibilidad de ciclos.

Todas las tuplas de la tabla de vecinos del nodo K son válidas y es el criterio de selección el que decide cuál es la mejor.

4.6.2. Criterio de Selección

A nivel de parametrización se definen k rangos de batería. En el primer rango r_k, va desde el máximo nivel de batería disponible, mientras que el último, r_1, incluirá la mínima batería disponible para la operación del nodo.

Sea R el conjunto de rangos de batería de cardinalidad k.

$R = [r_k, r_{k-1}, \ldots, r_i, \ldots, r_1)$

Donde, r_k es el máximo valor de energía provisto al nodo sensor, lr es la longitud de cada rango y de forma general $r_i = r_{i+1} - lr$, siendo $r_1 - lr$, el valor mínimo para realizar un ciclo de trabajo.

La cantidad de rangos k y la longitud de los intervalos lr son configurables de acuerdo a las características de las aplicaciones. Por ejemplo, si la aplicación requiere confiabilidad en la entrega, los rangos deben ser cuidadosamente definidos, ya que la batería de los nodos que participarán en el encaminamiento son un factor importante en la entrega del mensaje. Si por el contrario, la aplicación busca maximizar el ahorro de energía o minimizar el retraso en la entrega se puede definir un solo rango.

Los posibles caminos dentro de la tabla de vecinos son agrupados de acuerdo al rango de batería al que pertenece el nodo con valor mínimo dentro del camino.

El camino finalmente seleccionado es aquel con el mayor rango presente y que requiera la menor de cantidad de saltos para alcanzar a Sink. Es posible que varios caminos posean el mismo rango de batería y la misma cantidad de saltos, en este caso se toma en cuenta las métricas de calidad del enlace y se escoge aquel camino con mejores prestaciones.

Capítulo 5

Resultados experimentales

En este capítulo se reportan los resultados del estudio experimental realizado y que tuvo como objetivo comparar el desempeño del protocolo propuesto en este trabajo, *SHRP*, con otro protocolo de amplia aceptación. Para tal fin, se ha utilizado un simulador a nivel de paquetes que permitirá evaluar en diversos escenarios cada uno de los criterios de estudio.

Los modelos de simulación son una herramienta de muchísima utilidad para los diseñadores y administradores de sistemas, ya que permiten evaluar el comportamiento de un sistema antes de que sea puesto en operación. Diversas topologías y configuraciones pueden ser evaluadas a la hora de tomar una decisión sobre cual ofrece mejores resultados. Igualmente, los modelos de simulación son ampliamente utilizados en los procesos de reconfiguración y entonación para medir el impacto de una serie de cambios en los sistemas, sensores o protocolos sin tener que realizarlos sobre los sistemas de producción.

En la sección 5.1 se indica cuál es la herramienta seleccionada para realizar los

experimentos, una introducción sobre esta herramienta se ofrece en la sección 5.2. Luego, en la sección 5.3, se presenta la metodología utilizada. La sección 5.4 muestra la configuración del entorno de simulación. Posteriormente en 5.5 se describen los experimentos realizados con los resultados obtenidos y por último en la sección 5.6, se exponen algunas conclusiones derivadas de la experimentación.

5.1. Selección de la Herramienta para la simulación de Redes Inalámbricas de Sensores

El área de simulación de redes inalámbricas de sensores es un área relativamente nueva y actualmente en desarrollo. Sin embargo, son múltiples las herramientas de simulación ya existentes que podemos utilizar para simular el comportamiento de cientos de nodos para una aplicación o un protocolo específico. Se ha elegido NS-2 [34] ya que proporciona soporte a IEEE-802.15.4 a través de sus contribuciones y no sólo permite simular la tarjeta de radio CC2420 sino que también es posible simular el comportamiento de la red; incluye un modelo de simulación de gasto de energía y su código es libre. De hecho NS-2 es el estándar de facto para la simulación de redes en el área de investigación.

Quizás el punto desfavorable de NS-2 es que no permite simular las aplicaciones desarrolladas en NesC. Para tal fin, cuando se tengan disponibles programas en NesC es posible utilizar el simulador PowerTOSSIM. En el apéndice C se muestran las características principales de ésta y otras herramientas de simulación estudiadas donde se incluyen comentarios sobre sus ventajas y debilidades.

5.2. NS-2

NS (Versión-2) [34] es un simulador orientado a objetos basado en eventos discretos, desarrollado por el proyecto VINT en unión de esfuerzos con University of California Berkeley, University of Southern California/Information Sciences Institute (USC/ISI), Lawrence Berkeley National Laboratory (LBL) y Xerox PARC (Palo Alto Research Center). Fue escrito en C++ con una interfaz a los usuarios en OTcl [35]. El simulador soporta una jerarquía de clases en C++ (jerarquía compilada) y una jerarquía de clases similar en OTcl (jerarquía interpretada). Estas dos jerarquías están íntimamente relacionadas entre si. Desde el punto de vista de los usuarios, existe una correspondencia uno-a-uno entre cada una de las clases de la jerarquía interpretada y las de la jerarquía compilada.

El simulador de redes utiliza dos lenguajes debido a que considera que un simulador tiene dos tipos diferentes de cosas por hacer. Por un lado, para la simulación detallada de protocolos, requiere un lenguaje de programación que pueda manejar eficientemente bytes, encabezados de paquetes, y la implementación de algoritmos que se ejecutan sobre grandes conjuntos de datos. Para estas tareas, la velocidad en el tiempo de ejecución es más importante que el tiempo total que toma construir un escenario de simulación, el cual está compuesto por: ejecución de la simulación, encontrar el error, arreglar el error, recompilar y volver a ejecutar.

Por otro lado, gran parte de la investigación en redes requiere de pequeñas variaciones de parámetros o configuraciones, o una rápida exploración a un buen número de escenarios. En estos casos, el tiempo de interacción (cambiar el modelo y volver a ejecutar) es más importante. Dado que el ajuste al protocolo en estos casos se realiza

una sola vez (al comienzo de la simulación) el tiempo de ejecución de dicha parte es menos importante.

NS logra estas dos necesidades con dos lenguajes, C++ y OTcl. C++ es rápido para ejecutar pero lento para cambiar, siendo el más indicado para la implementación detallada de protocolos. OTcl ejecuta mucho más lento pero puede ser cambiado muy rápidamente (e interactivamente), siendo el ideal para la configuración de la simulación. NS (usando tclcl [35]) provee los mecanismos para que los objetos y variables aparezcan en ambos lenguajes.

La interfaz de tcl puede ser usada cuando se trata de pequeños cambios en los escenarios que pueden ser fácilmente implementados. De forma similar, utilizando C++ se puede implementar cambios que involucran el procesamiento de todos los paquetes entrantes, o cuando se puede anticipar cambios en el comportamiento del protocolo.

En NS, el transcurrir del tiempo se simula al indicar el momento en que los eventos deben ser ejecutados. El control de dicha ejecución es mantenida por el planificador. Un evento es un objeto en la jerarquía C++ con: un identificador único, un tiempo planificado y un apuntador a un objeto que maneja el evento. El planificador mantiene una estructura de datos ordenada, con los eventos que serán ejecutados y los dispara uno por uno, invocando al manejador del evento que tenga asociado.

5.3. Metodología

El protocolo seleccionado para realizar las comparaciones versus *SHRP* es *Directed Diffusion (DD)*, debido a que es uno de los más citados entre los protocolos de redes de

sensores. Tal como es reportado en el estudio de [11], son diversas las publicaciones que hacen referencia a este protocolo así como a sus algoritmos de difusión 1PP, 2PP y Push que brevemente fueron comentados en 3.1.4. Entre estos algoritmos se ha seleccionado One Phase Pull, dado que es el más conveniente para topologías con múltiples transmisores y un solo receptor [13] similares al entorno de estudio de este trabajo. Dado que en ambos protocolos es posible aplicar criterios de agregación de datos y que en *DD* no están implementados, se ha preferido no incluir políticas de agregación en *SHRP* durante este estudio.

Son cuatro los criterios seleccionados para analizar el desempeño de *SHRP* y realizar las comparaciones: consumo de energía, confiabilidad en la entrega de los datos, tiempo de convergencia y sobrecarga de mensajes de control. Los dos primeros fueron seleccionados ya que corresponden a dos métricas del protocolo propuesto. El tiempo de convergencia muestra cuánto le toma al protocolo descubrir la topología y adaptarse a los cambios, y por último el estudio de los mensajes de control permite determinar la sobrecarga que requiere *SHRP*, en mensajes propios del protocolo,

- Sobrecarga de mensajes de Control: Mide la tasa de mensajes específicos del protocolo de encaminamiento que son enviados durante la simulación. Esta métrica permite establecer el costo que adiciona el protocolo de encaminamiento al transmitir los datos. En los experimentos realizados se unen los mensajes de control y los de datos de *SHRP* ya que *DD* los maneja juntos. Dado que la tasa de transmisión de datos y el tamaño del paquete es el mismo, esto no afectará los resultados cualitativos.
- Consumo de energía: Mide la energía consumida por los nodos de la red. Esta métrica nos da una idea del trabajo realizado por los nodos para entregar los

mensajes a Sink. Se mide también la desviación estándar de la energía gastada con lo que se determina el consumo simétrico de energía ya que esto es importante para mantener el tiempo de vida de la red.

- Confiabilidad en la entrega de los datos: Mide durante la simulación los paquetes que son descartados por los nodos. Dado que se realizan los experimentos utilizando los mismos parámetros, esta métrica nos indica en términos de paquetes la eficiencia del protocolo para entregar los mensajes a Sink.

- Tiempo de Convergencia: Mide el tiempo que le lleva al protocolo construir y mantener su árbol de rutas posibles. Mientras no se alcanza dicha convergencia, los nodos coordinadores no disponen de rutas para enviar los paquetes, descartando los paquetes de datos que reciben y deteniendo el flujo de información hacia Sink. En el caso de protocolos como *DD*, también afecta el envío de datos ya que los nodos sensores solo envían información una vez que la red ha convergido.

Para estudiar el consumo de energía se ha utilizado el modelo que provee NS-2. Éste requiere una batería inicial para cada nodo y el consumo necesario para transmitir y para recibir. Se han utilizado los datos de consumo reales del chip de radio CC2420 [50]. En cuanto a la batería inicial de los nodos, se ha utilizado un valor bastante pequeño para poder apreciar los cambios en el rango de batería de los nodos propuestos por el protocolo *SHRP* durante el tiempo de simulación.

5.4. Entorno de Simulación

El estudio de desempeño de *SHRP* se realiza en función al tamaño de la red. Los parámetros más importantes considerados durante la simulación son presentados en la tabla 5.1. Los nodos son desplegados en un área rectángular de 50m por 100m en forma de malla o grid, separando cada uno de los nodos a 10 metros tanto de los nodos que se encuentran a su izquierda y derecha, como de los que tiene arriba y abajo. Este tipo de topologías son más exigentes en cuanto al tiempo de convergencia de la red al presentar equidistancia y estar por debajo del alcance máximo de transmisión, factor importante para este estudio dado que es uno de los criterios analizados.

Tipo	Parámetros	Valor
Generales	Área Utilizada (mts.)	50 x 100
	Candidad de Nodos	según el experimento (10,20,50,100)
	tiempo de estabilización previo(segs.)	60
	Tiempo Simulación (segs.)	300
	Intervalo transmisión de datos (segs.)	2
	Retraso en reenvío (mseg.)	30
	Tamaño del Paquete de datos (bytes)	40
Batería	Batería Inicial (Joules)	0.5
	Batería Mínima de operación(Joules)	0.3
Radio IEEE 802.15.4	Frecuencia (MHz)	914
	Voltaje (V)	3
	Consumo energía transmisión (mAmp)	12
	Consumo energía recepción (mAmp)	8
	Alcance de la Antena (mts)	15

Tabla 5.1: Variables utilizadas en el Entorno de Simulación

En la figura 5.1 se aprecia un ejemplo de la distribución de los nodos donde el nodo Sink siempre se coloca en el centro del borde inferior del área de estudio.

El simulador NS-2 implementa la capa física y la capa MAC de IEEE 802.15.4. Los experimentos se han configurado de forma tal que solo existe un nodo coordinador PAN

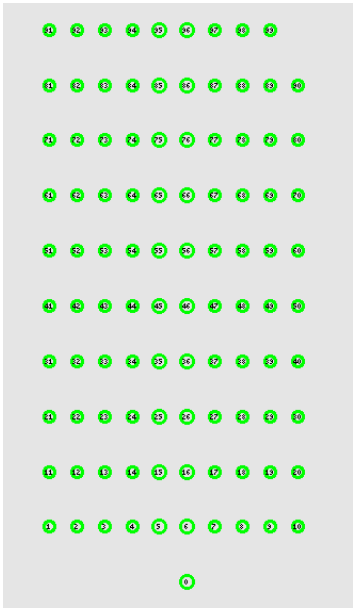

Figura 5.1: Ejemplo del tipo de topología en forma de malla utilizada en los experimentos

(Personal Area Network) utilizando una modalidad sin beacons (CSMA-CA no ranurado) y los demás nodos son dispositivos FFD (Full Functional Devices), que además de ser coordinadores permiten que otros nodos se asocien con ellos [1].

Cada uno de los experimentos son realizados para 10, 20, 50 y 100 nodos. Cada nodo tiene un alcance de radio de 15 metros. Se hace de esta forma para mantener constante la densidad de los nodos. El tráfico durante las simulaciones es constante, se escogen tres de los nodos más alejados al nodo Sink para que transmitan datos periódicamente cada 2 segundos.

El tiempo total de cada experimento es de 300 segundos, con un tiempo de estabilización previo (warm up) de 60 segundos. La carga útil de los paquetes de datos es de 40 bytes y se transmite un paquete cada 2 segundos.

[1] Se ha utilizado el release 29 de ns-2, éste o releases más recientes pueden ser descargados de `http://www.isi.edu/nsnam/ns`

En la tabla 5.2 se presentan los valores específicos de la configuración de ambos protocolos. En el caso de *DD*, fue necesario modificar su implementación para reducir el tamaño de los paquetes que genera debido a que utilizan, innecesariamente, representaciones muy grandes para los datos que se desean trasmitir, afectando el consumo de energía necesario para su transmisión y recepción. Es importante hacer notar que con cada paquete de datos se transmiten todos los datos del interés, los cuales se han reducido a su mínima expresión. Para reducir las colisiones en la transmisión de mensajes NMI, se ha utilizado una fórmula similar a la que utiliza Directed Diffusion para transmitir sus mensajes de Interés3.1.4 que introduce un valor aleatorio al intervalo parametrizado.

SHRP		*DD*	
Parámetro	Valor	Parámetro	Valor
Intervalo NMI (seg.)	30	Período Interés (seg.)	30
Retraso Reenvio NMI (mseg.)	30	Retraso reenvio Interés (mseg.)	30
Intervalo HELLO (seg.)	15	Algoritmo	One-Phase-Pull
# rangos Energía	3		

Tabla 5.2: Parámetros de Configuración Específicos para *SHRP* y *Directed Diffusion*

5.5. Experimentos Realizados

En esta sección, se presentan los experimentos realizados siguiendo la metodología comentada previamente. Se ejecutaron simulaciones que fueron configuradas específicamente para cada uno de de los criterios seleccionados.

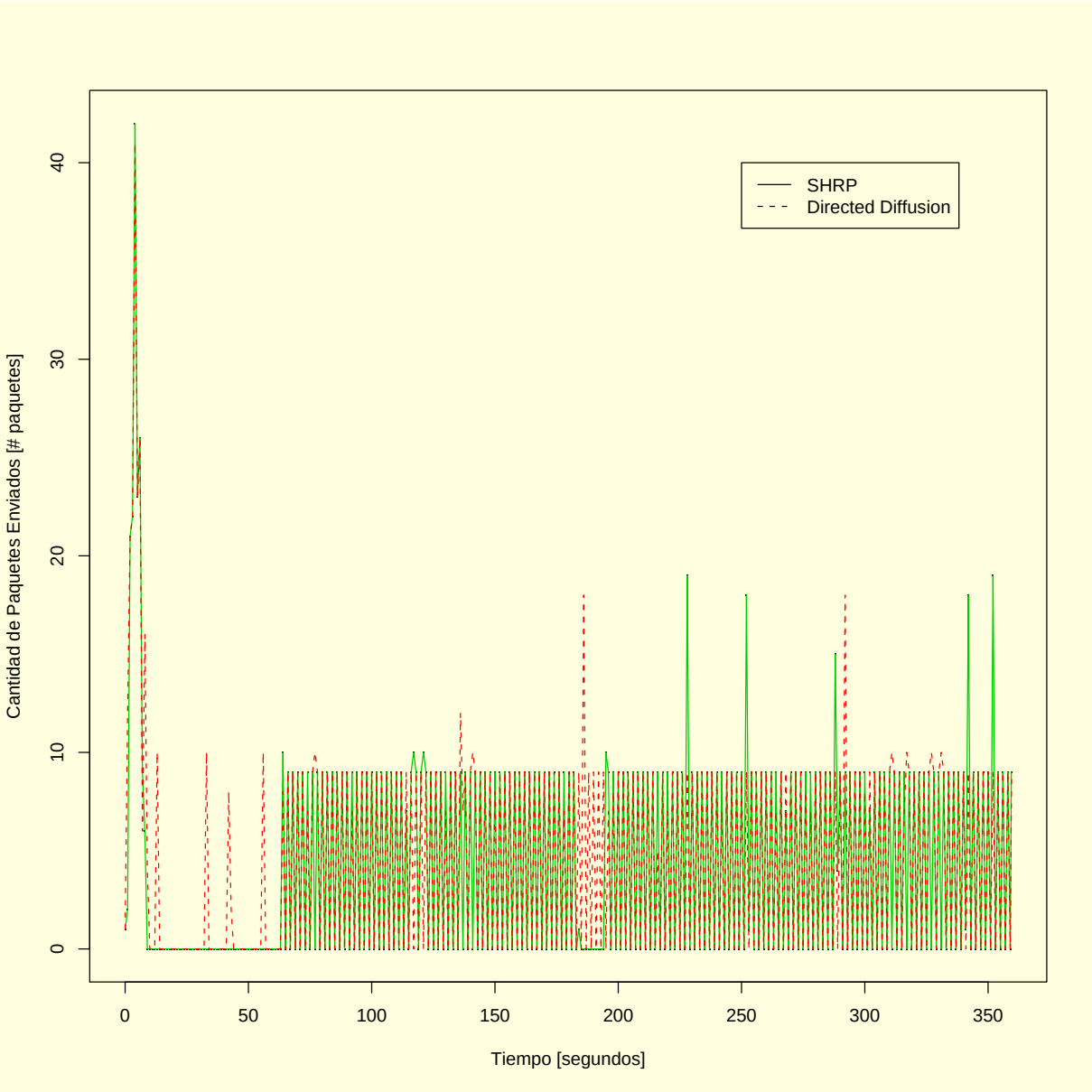

Figura 5.2: Comparación de los mensajes transmitidos por *SHRP* y *Directed Diffusion* para 10 nodos

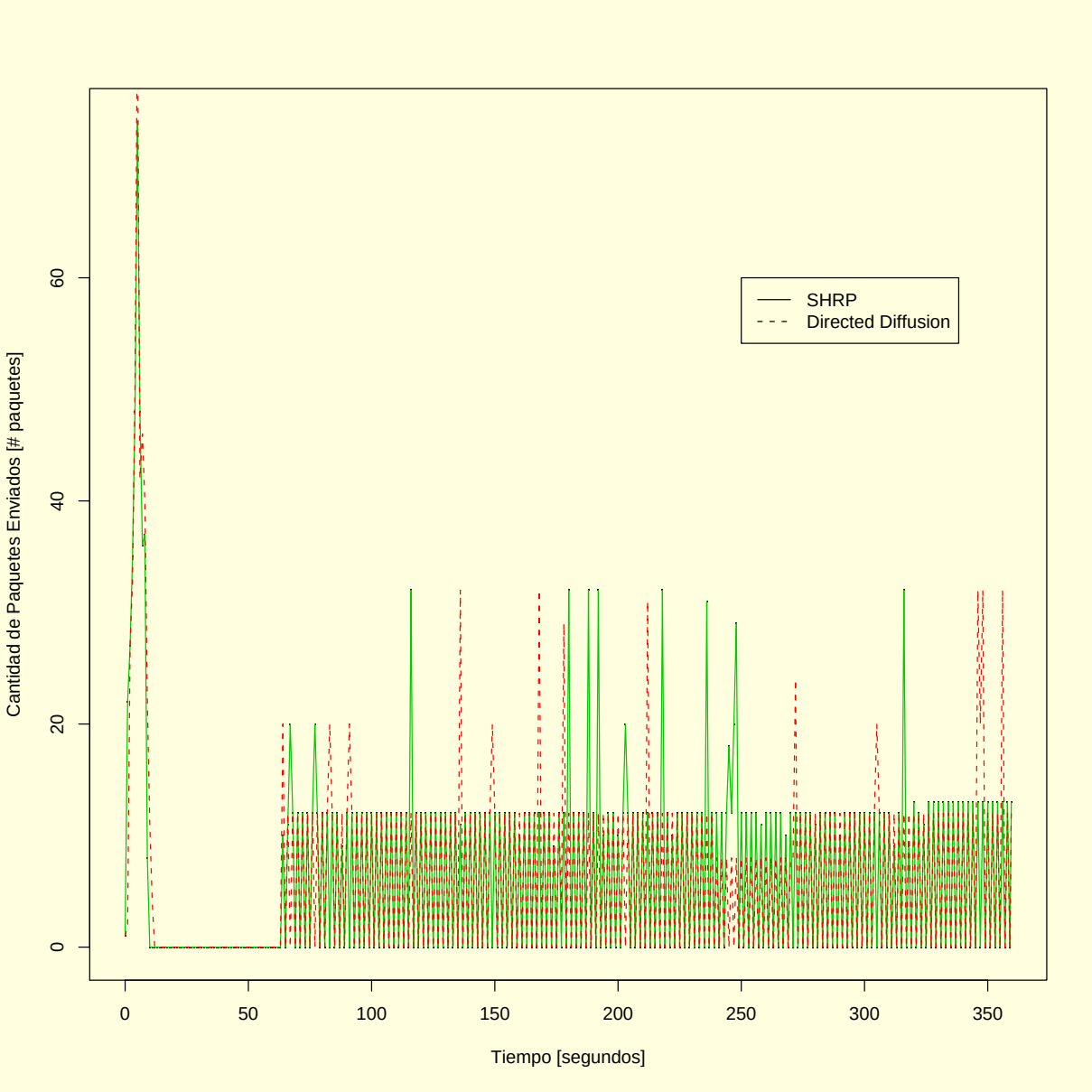

Figura 5.3: Comparación de los mensajes transmitidos por *SHRP* y *Directed Diffusion* para 20 nodos

Sobrecarga de Mensajes de Control

Al evaluar los paquetes enviados en las figuras 5.2, 5.3, 5.4 y 5.5, se puede apreciar como el comportamiento de ambos protocolos es similar, sobreponiéndose en muchas ocasiones una curva sobre otra. Gran parte del tiempo de simulación presenta un tráfico constante que corresponde a la transmisión de datos y los picos corresponden al envío de NMI y del interés para *SHRP* y *DD* respectivamente.

En cuanto al tiempo de convergencia, *DD* puede requerir más de un envio de interés para lograr alcanzar a todos los nodos. En la figura 5.5 se puede ver como no pudo lograr la convergencia antes de los 100 segundos por lo que no hubo tráfico de datos durante el periodo 60 a 100 segundos. Algo similar se puede apreciar en el gráfico 5.4 luego de los 300 segundos. Por su parte, *SHRP* tuvo un tiempo de convergencia muy similar independientemente del número de nodos de la topología, lo que significa que escala mejor con sus mensajes de control.

# Nodos	Cant. de Mensajes Enviados	
	SHRP	*DD*
10 Nodos	1363	1450
20 Nodos	1770	1981
50 Nodos	4789	3792
100 Nodos	5081	4871

Tabla 5.3: Cantidad de Mensajes Enviados en cada experimento

Al verificar el total de mensajes enviados en la tabla 5.3, *SHRP* envía menor cantidad de mensajes para 10 y 20 nodos. Para 50 y 100 nodos debemos considerar que *DD* envió menos datos debido a la falta de convergencia de la red por lo que si se resta el tráfico transmitido durante ese periodo por *SHRP* sus valores son mejores que *DD*. Las mejoras al disminuir la cantidad de mensajes no solo contribuyen a obtener un buen

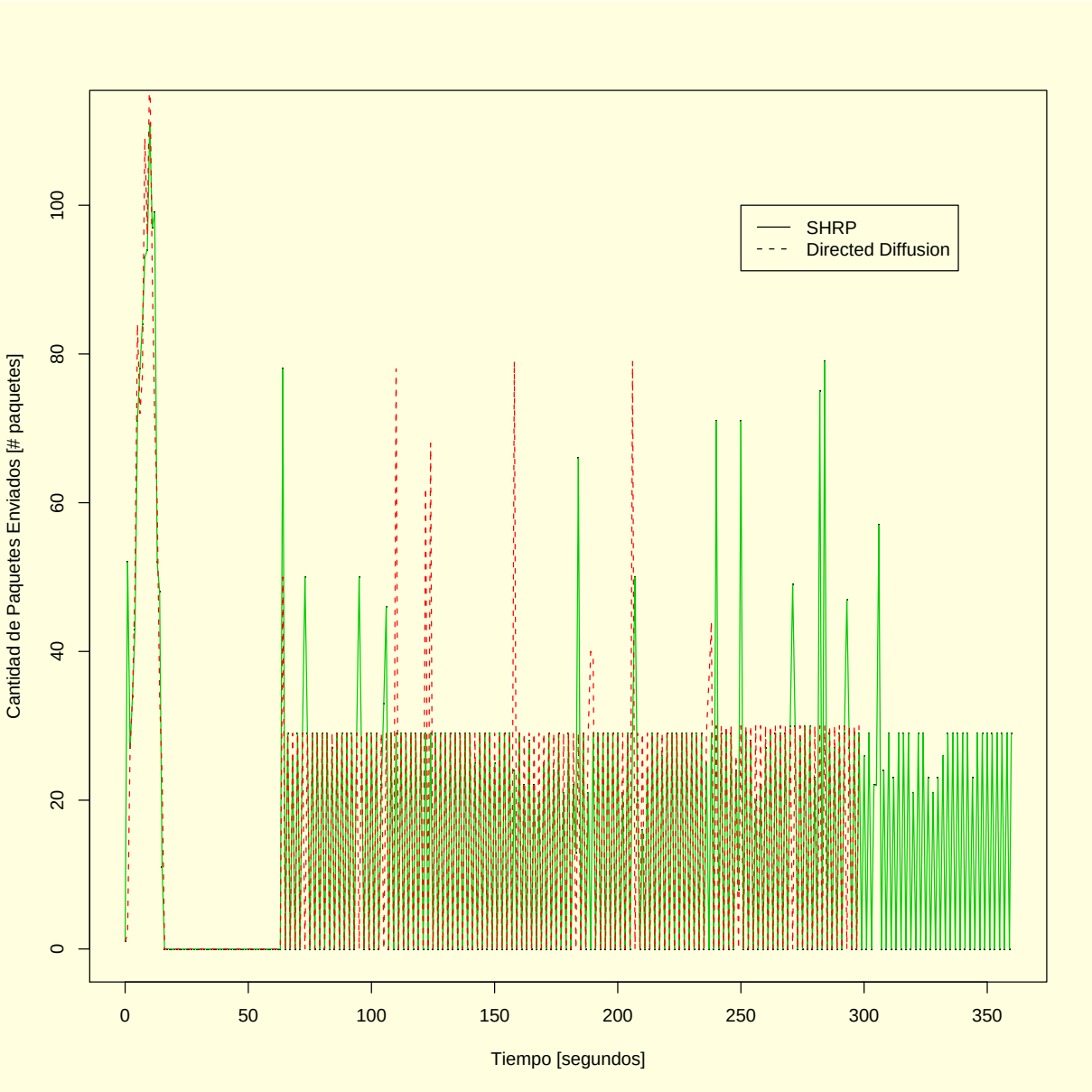

Figura 5.4: Comparación de los mensajes transmitidos por *SHRP* y *Directed Diffusion* para 50 nodos

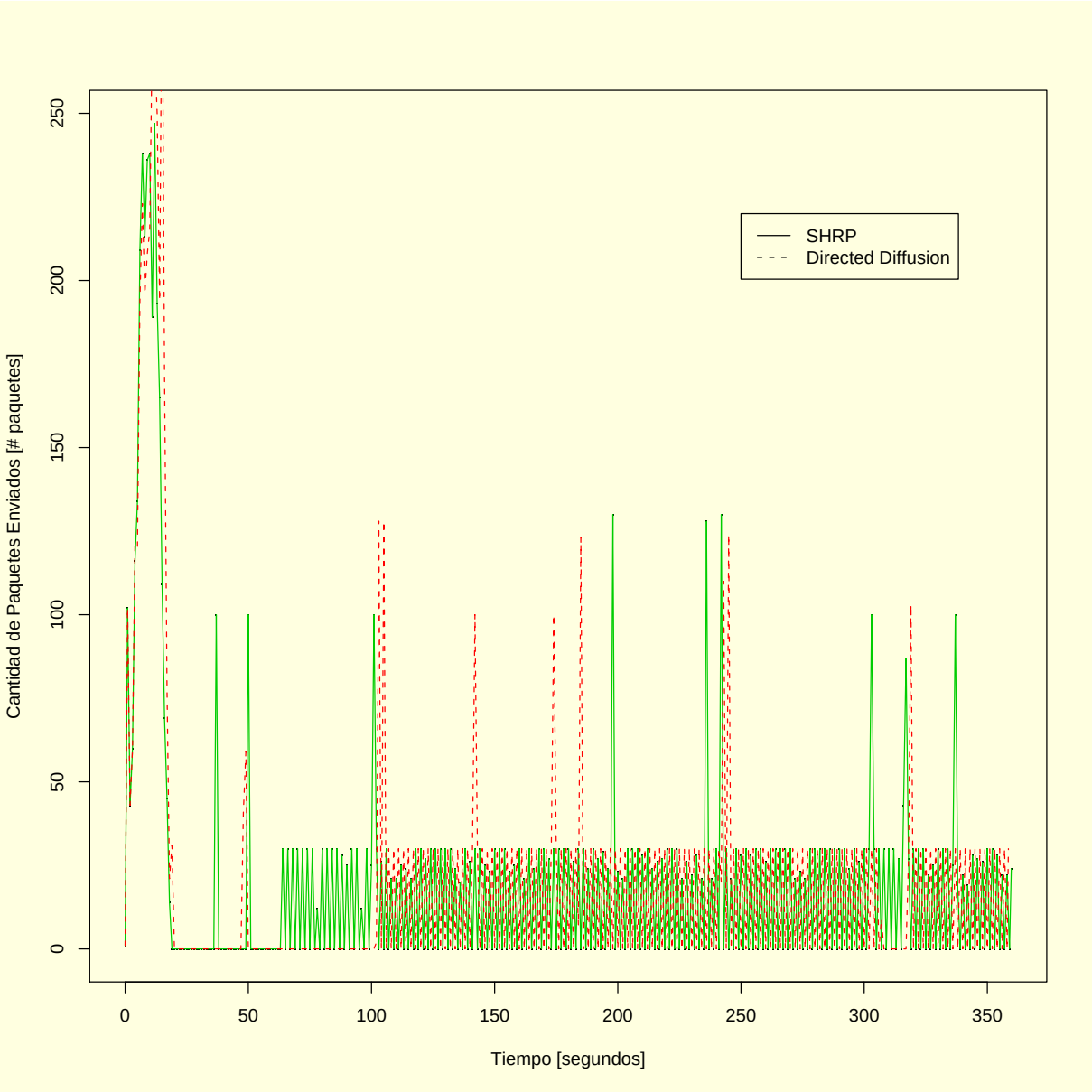

Figura 5.5: Comparación de los mensajes transmitidos por *SHRP* y *Directed Diffusion* para 100 nodos

tiempo de convergencia, también representan un ahorro en el ancho de banda y como veremos más adelante también implican un ahorro de energía.

Confiabilidad en la Entrega

En estos experimentos se toma en cuenta los mensajes de control y datos que han sido descartados en cada uno de los protocolos. Como ya se mencionó anteriormente se han considerado los mensajes de control debido a que *DD* los maneja conjuntamente con los datos y no hay forma de diferenciarlos. Sin embargo, dado que el entorno de simulación es el mismo, incluyendo el tráfico, dicha inclusión no modifica la tendencia de los resultados. También es importante destacar que en *DD* los nodos sensores solamente transmiten información cuando tienen suscriptores asociados. Dicha suscripción se realiza al recibir el mensaje de interés, por lo que al dejar de recibir estos mensajes durante un período determinado los nodos dejarán de transmitir. Por esta razón al estudiar los mensajes descartados, se debe tomar en cuenta el porcentaje de mensajes pérdidos en relación a los enviados (PPE) ya que a pesar que se busca una mínima cantidad de descartes, lo principal es maximizar la cantidad de paquetes de datos transmitidos.

Tal y como sugieren los gráficos de la figuras 5.6, 5.7, 5.8 y 5.9 *DD* descarta más paquetes en todos los experimentos, en la tabla 5.4 se puede comprobar el total de mensajes descartados en cada caso y como la diferencia del PPE entre ambos protocolos aumenta considerablemente al aumentar la cantidad de nodos. Con estos resultados se aprecia como *SHRP* tuvo mayor confiabilidad en la entrega de paquetes, métrica importante para protocolo, sin que esto genere mayor impacto en términos de energía como se verá más adelante.

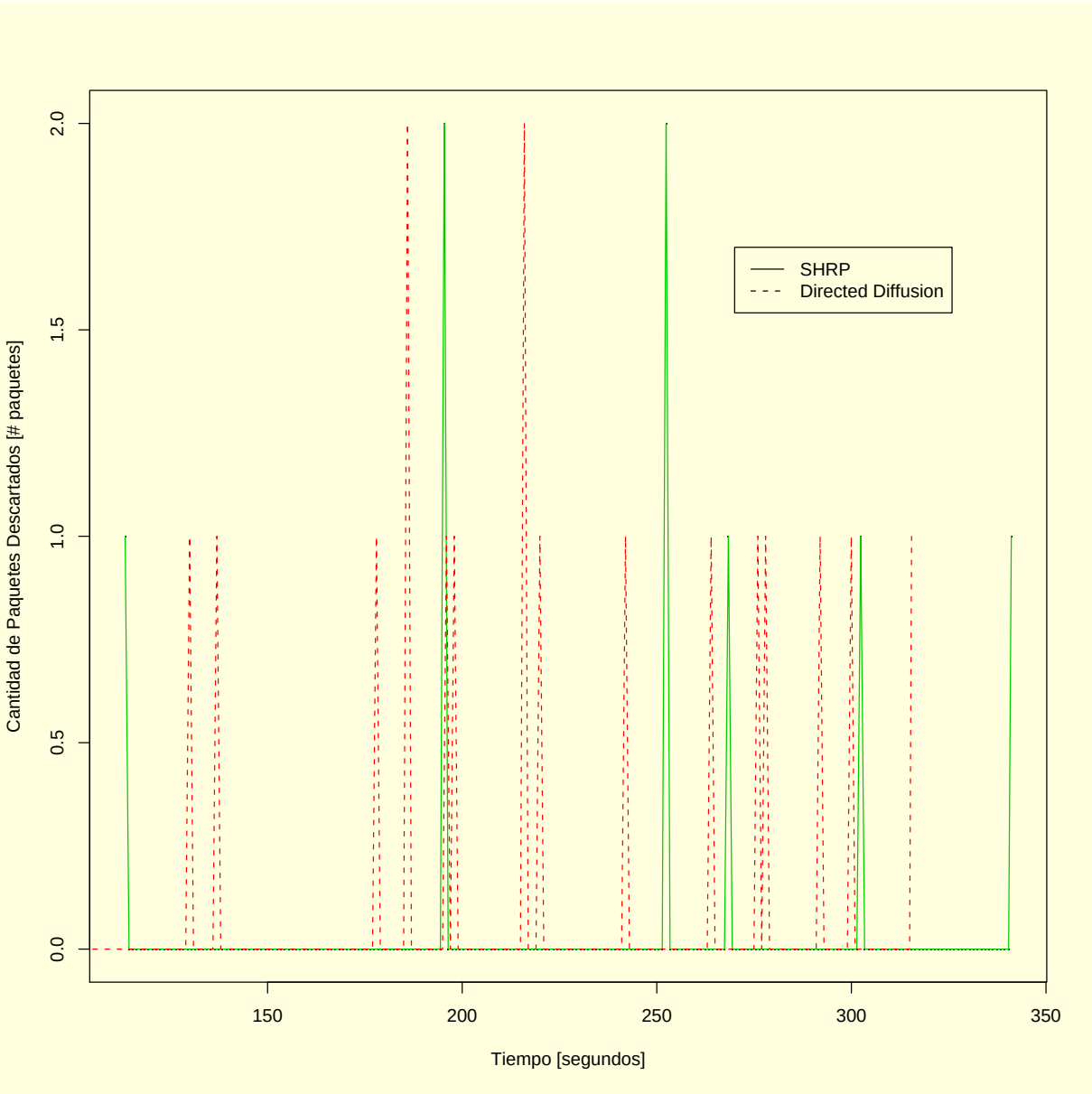

Figura 5.6: Comparación de los mensajes descartados por *SHRP* y *Directed Diffusion* para 10 nodos

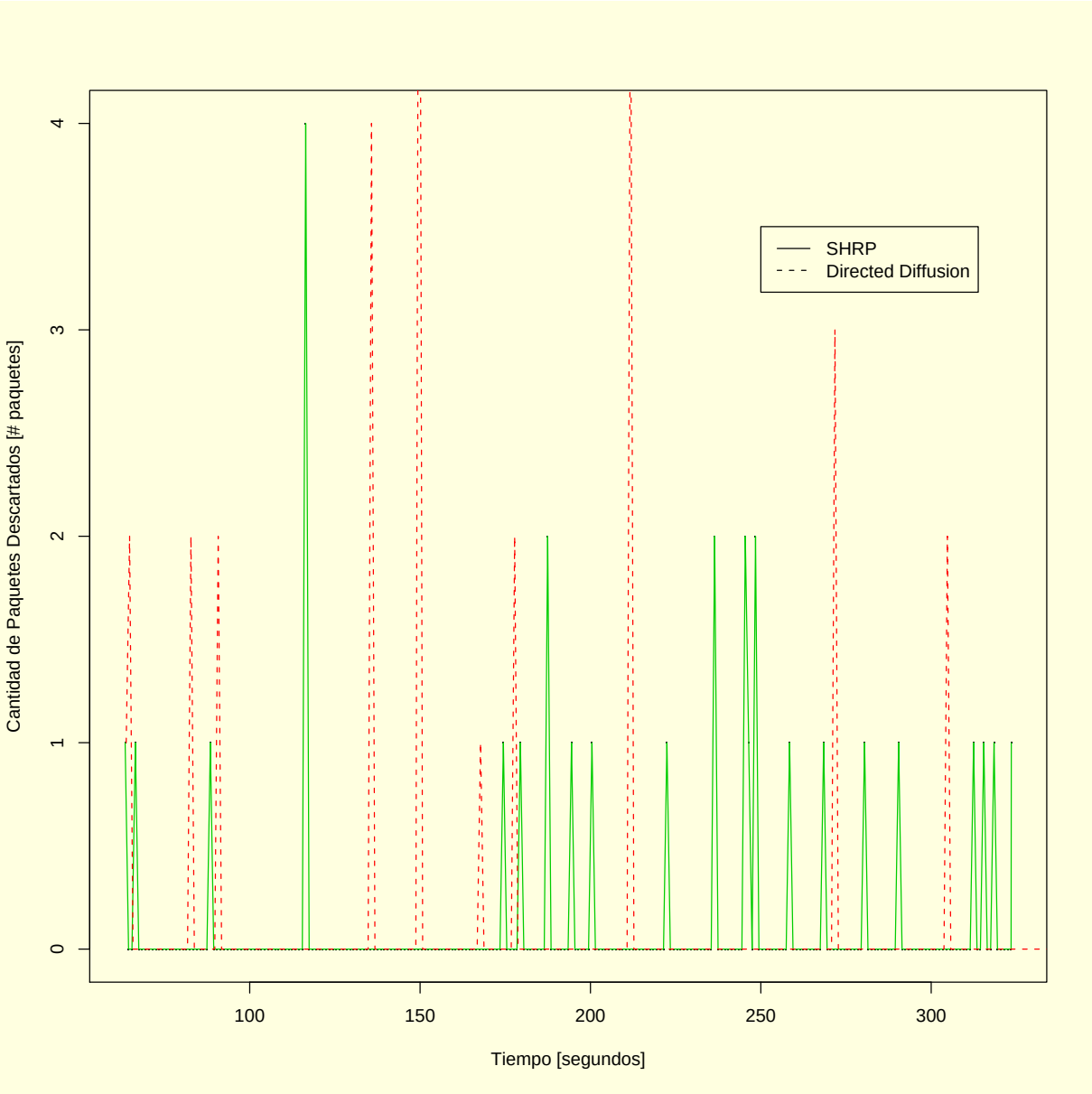

Figura 5.7: Comparación de los mensajes descartados por *SHRP* y *Directed Diffusion* para 20 nodos

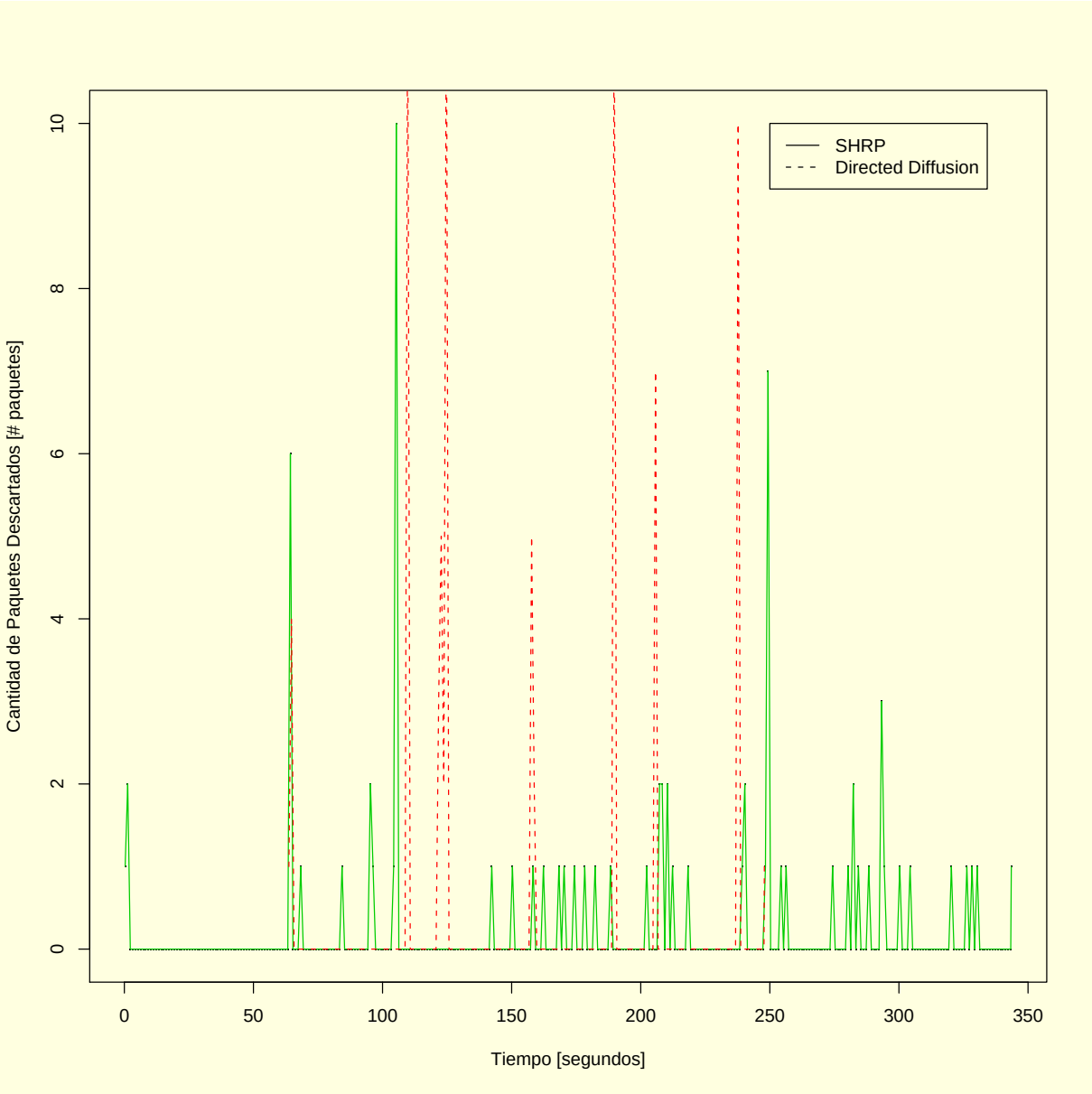

Figura 5.8: Comparación de los mensajes descartados por *SHRP* y *Directed Diffusion* para 50 nodos

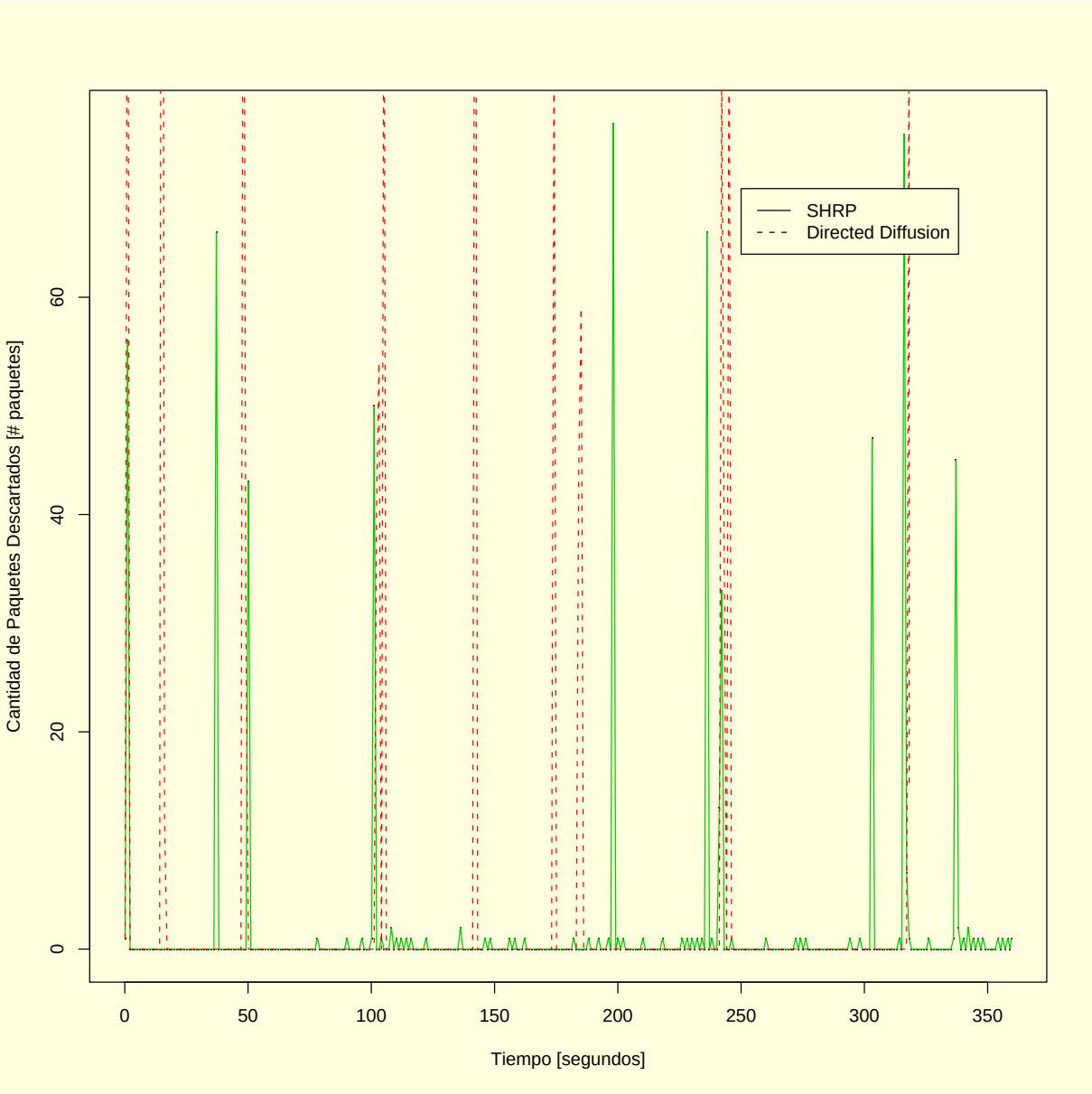

Figura 5.9: Comparación de los mensajes descartados por *SHRP* y *Directed Diffusion* para 100 nodos

A pesar que la energía inicial es muy pequeña, no lo es tanto como para que los nodos salgan de la red por falta de energía. Para evaluar la confiabilidad de entrega en una situación límite se realizó un experimento adicional para la topología de 50 nodos, que reportó mayor igualdad entre ambos protocolos. En dicho experimento se modificaron dos parámetros con respecto a los demás experimentos: la energía inicial del nodo a 0.02 Joules y la energía mínima de operación a 0.005 Joules.

Para tener una idea del esfuerzo al que se sometió a los protocolos, al finalizar la simulación 18 nodos dejaron de operar en *DD* por 36 nodos en *SHRP*. En las figuras 5.10 y 5.11 se presentan los paquetes enviados y descartados durante este experimento para ambos protocolos. En la figura 5.10 se puede ver como *DD* mantiene un tráfico constante hasta los 136 segundos, luego el tráfico se mantiene con altibajos hasta los 186 segundos hasta que deja de trasmitir paquetes de datos a los 243 segundos. Esto se debe a que se vence la información de interés que poseen los nodos que generan los datos y al no conseguir mantener la topología para que reciban nuevos mensajes de interés dejan de transmitir información. *SHRP* por su parte, mantiene la transmisión de datos sin mayores pérdidas hasta los 260 segundos, 74 segundos más que *DD*. Manteniendo la entrega de mensajes por más tiempo a pesar de las caídas de los nodos.

En la figura 5.11 se puede apreciar como *DD* pierde gran cantidad de paquetes a

# Nodos	*SHRP*		*DD*	
	M.Descartados	PPE	M.Descartados	PPE
10 Nodos	8	0.58	25	1.72
20 Nodos	29	1.63	39	1.96
50 Nodos	74	1.54	76	2.00
100 Nodos	634	12.47	1296	26.60

Tabla 5.4: Suma de los Mensajes de Control y de Datos Descartados en cada experimento

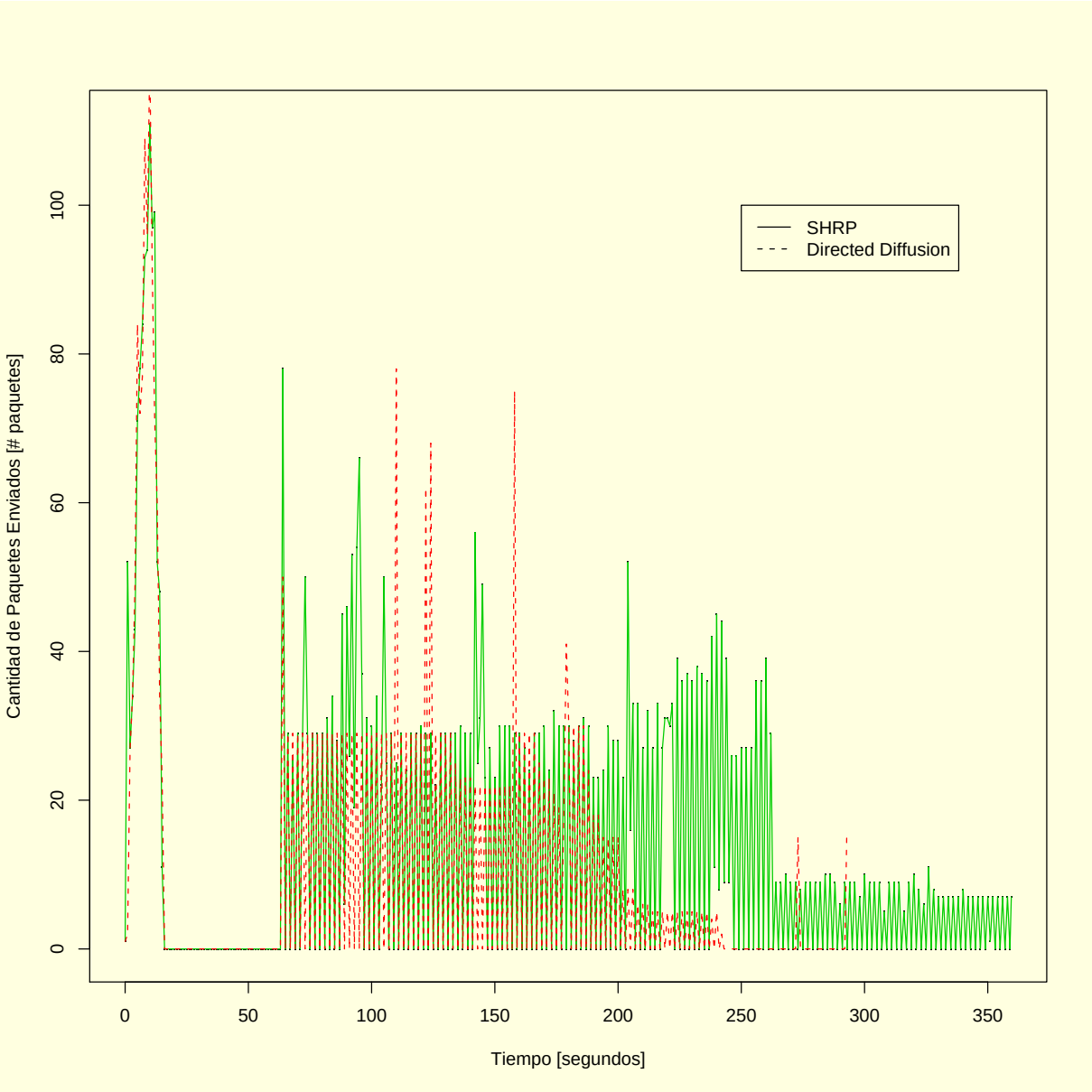

Figura 5.10: Comparación de los mensajes enviados por *SHRP* y *Directed Diffusion* para 50 nodos con Mínima energía disponible

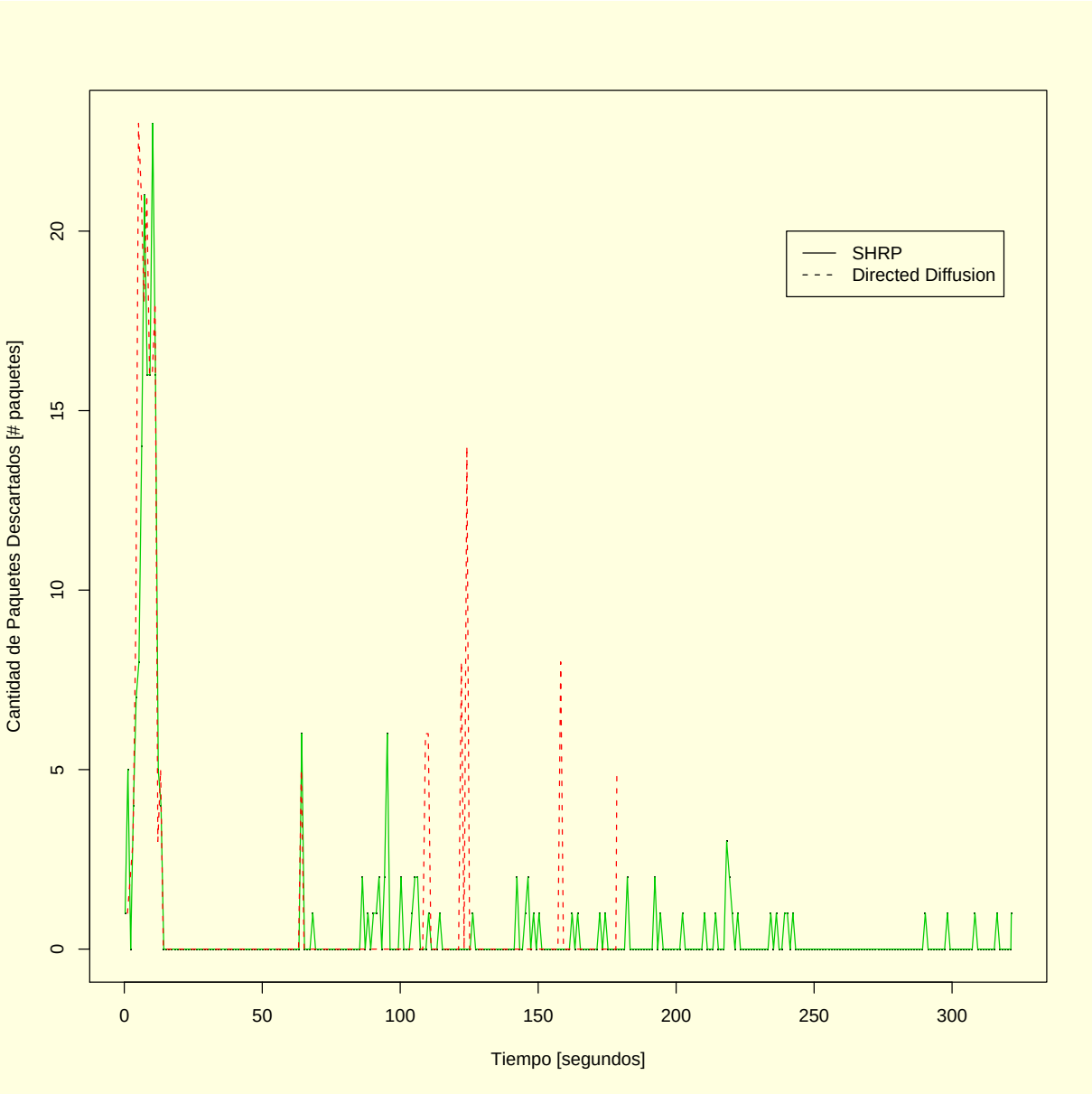

Figura 5.11: Comparación de los mensajes descartados por *SHRP* y *Directed Diffusion* para 50 nodos con Mínima energía disponible

los 124 segundos y luego a los 160 segundos, para posteriormente perder la conectividad de la red dejando de transmitir. Las pérdidas presentadas por *SHRP* son generadas en su mayoría por los mensajes Hello generados al presentarse cambios de encaminamiento frecuentes por la disminución de energía y que eventualmente pueden generar algunas colisiones en la red.

Consumo de Energía

Con este estudio, se evaluará el consumo de energía durante el tiempo de simulación. En todos los casos los nodos parten con una misma cantidad de energía inicial, con lo cual podremos evaluar la simetría en el consumo de energía de los nodos.

Las gráficas de las figuras 5.12, 5.13, 5.14 y 5.15 muestran como *SHRP* es más eficiente en el gasto de energía a pesar que está interesado en la confiabilidad del mensaje. Una de las razones de esta diferencia se debe a que genera menor cantidad de mensajes como se pudo ver en las figuras 5.2, 5.3, 5.4 y 5.5. También hay que considerar el tamaño del encabezado de control de *SHRP* el cual es bastante pequeño (explicado en detalle en la sección 4.4), para no incrementar demasiado el paquete de datos que es transmitido.

# Nodos	*SHRP*		*DD*	
	Prom. Disponible	Desv. Estándar	Prom. Disponible	Desv. Estándar
10 Nodos	0.475856	0.008058	0.461130	0.013125
20 Nodos	0.480700	0.007816	0.468433	0.011973
50 Nodos	0.479682	0.009452	0.473689	0.010476
100 Nodos	0.476089	0.007719	0.464481	0.008935

Tabla 5.5: Promedio de Bateria Disponible y Desviación Stándar para cada Experimento

Sin embargo el resultado más importante se presenta en la tabla 5.5, que presenta

el promedio de energía disponible en cada experimento, siendo *SHRP* mejor en todos los experimentos, y la desviación estándar que valora la uniformidad en el consumo de energía y donde *SHRP* obtiene mejores prestaciones, alargando la vida de la red y manteniendo por mayor tiempo caminos confiables para el envío de mensajes, el cual es uno de los objetivos trazados por el protocolo.

5.6. Resultados

De acuerdo a los resultados obtenidos a partir de las simulaciones para cada uno de los criterios de evaluación, se puede concluir:

- *SHRP* tiene potencial para ofrecer eficiencia en términos de energía. No solo por reducir el consumo total de energía al enviar menos mensajes de control y tener un encabezado más pequeño, sino que también logra que este consumo se distribuya de forma más equitativa entre los nodos. Esta distribución en el consumo permite que se mantengan caminos confiables por mucho más tiempo garantizando de este modo mayor confiabilidad en la entrega de mensajes.
- Con *SHRP* la red converge de manera escalable y rápida a la hora de mantener la topología de la red. Mostrandose mejor que *Directed Diffusion* en caso de caída de nodos por falta de baterías y en situaciones de interferencia.
- Al envíar menos mensajes de control también ahorra en ancho de banda y disminuye la probabilidad de colisiones en la red, además de ahorrar energía.
- La posibilidad de configurar los rangos de energía le permite a *SHRP*, ser flexible para distintos tipos de aplicaciones. Es posible disminuir la confiabilidad de

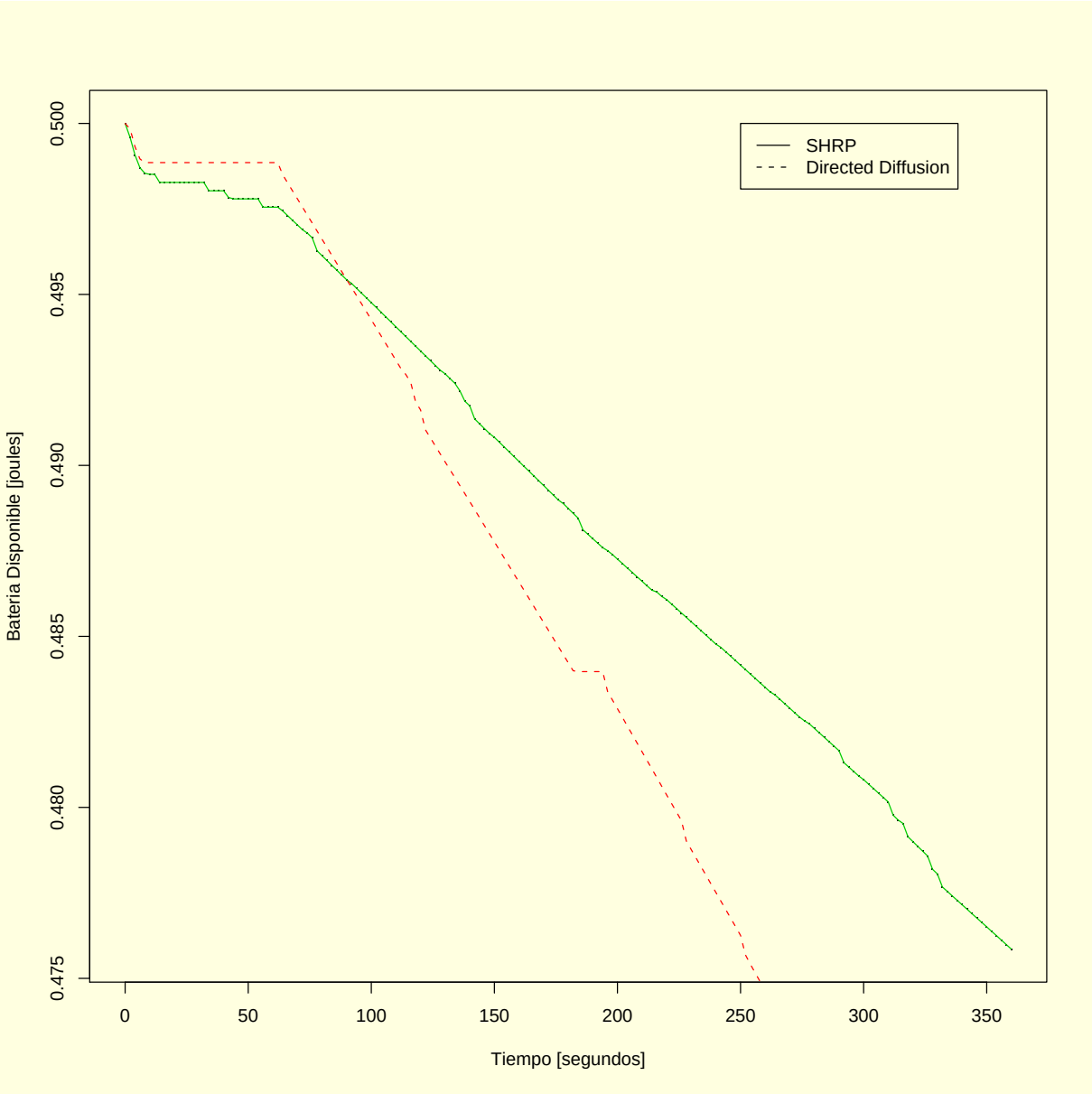

Figura 5.12: Comparación del consumo de bateria utilizando *SHRP* y *Directed Diffusion* para 10 nodos

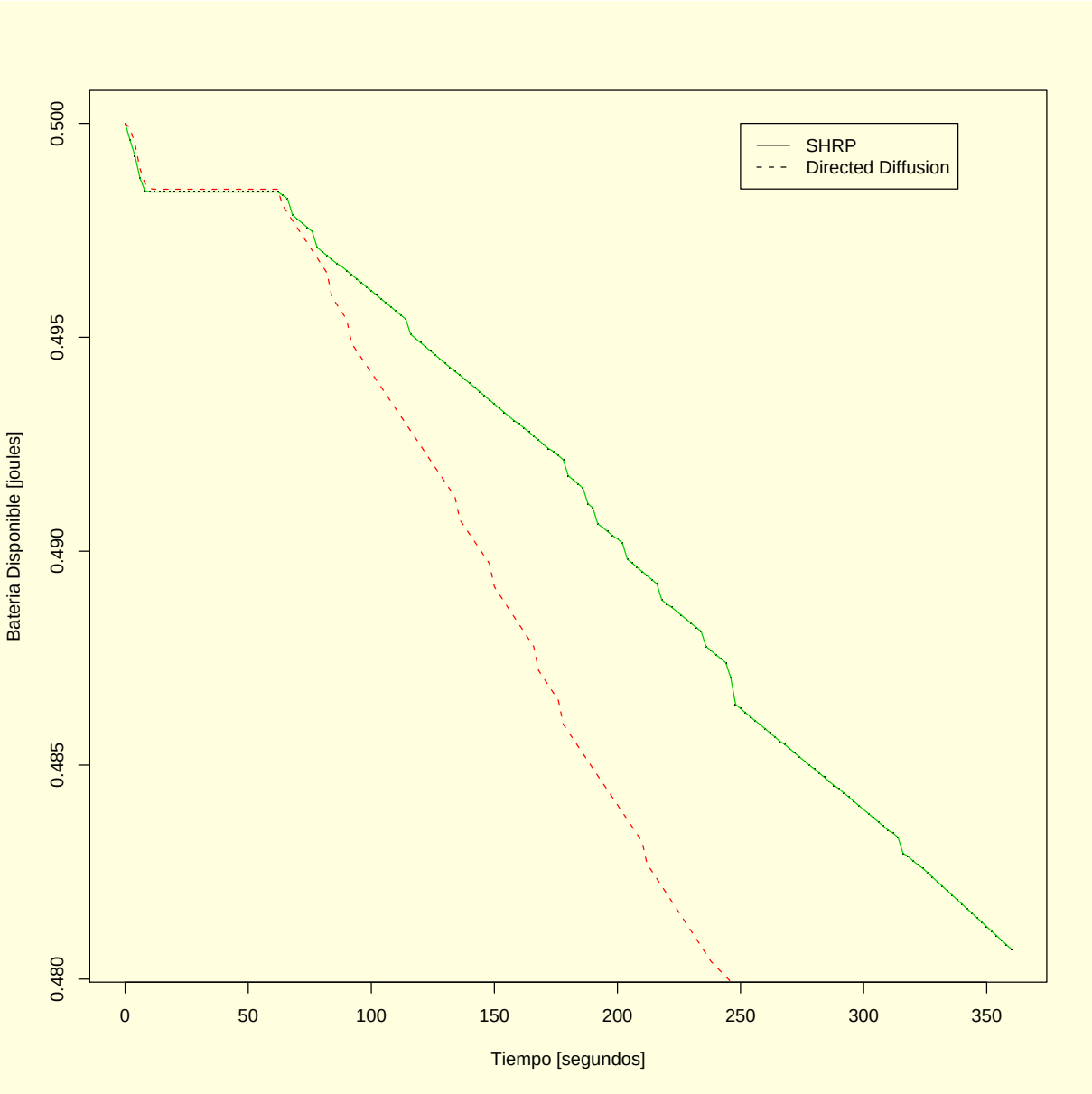

Figura 5.13: Comparación del consumo de bateria utilizando *SHRP* y *Directed Diffusion* para 20 nodos

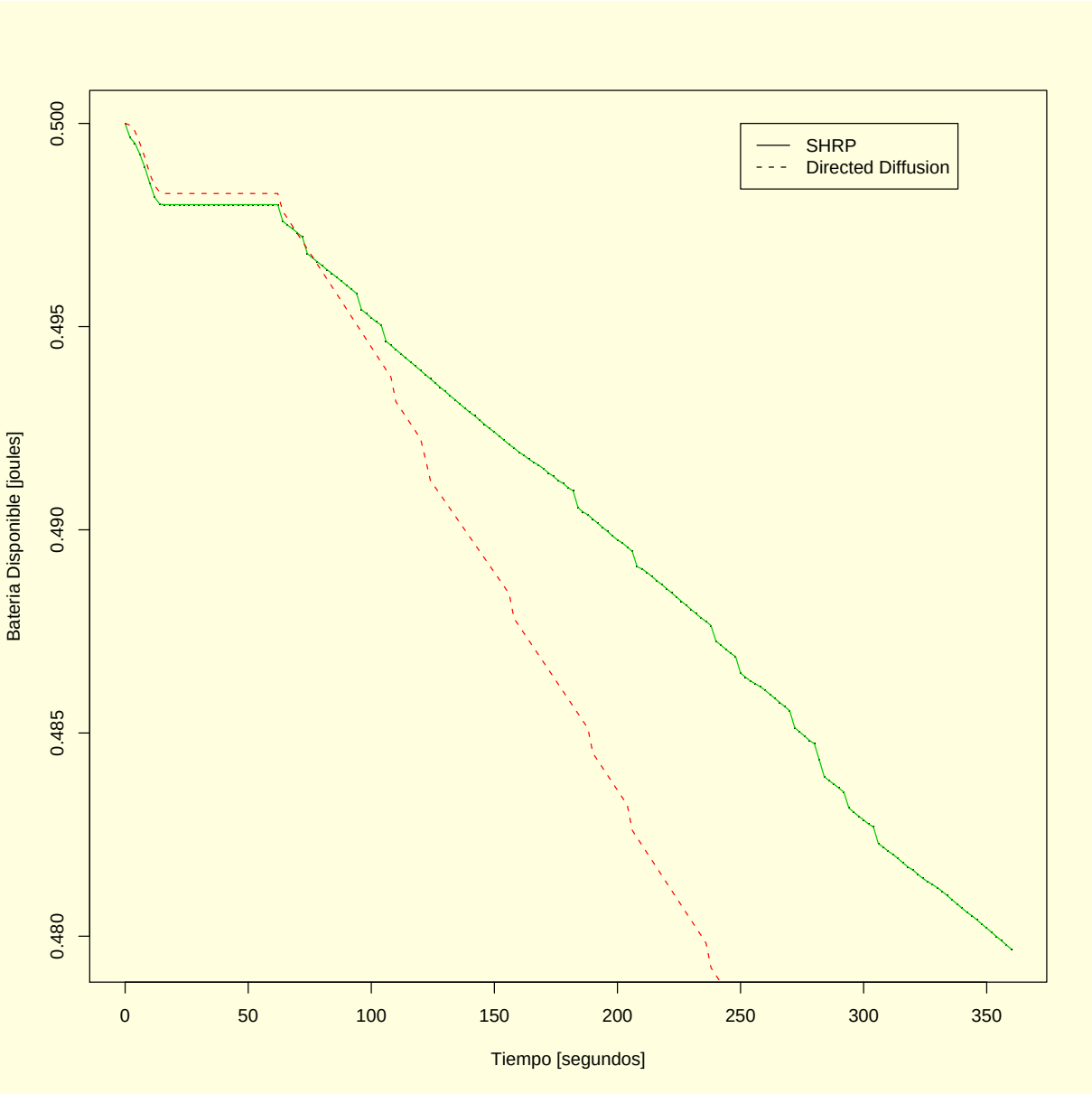

Figura 5.14: Comparación del consumo de bateria utilizando *SHRP* y *Directed Diffusion* para 50 nodos

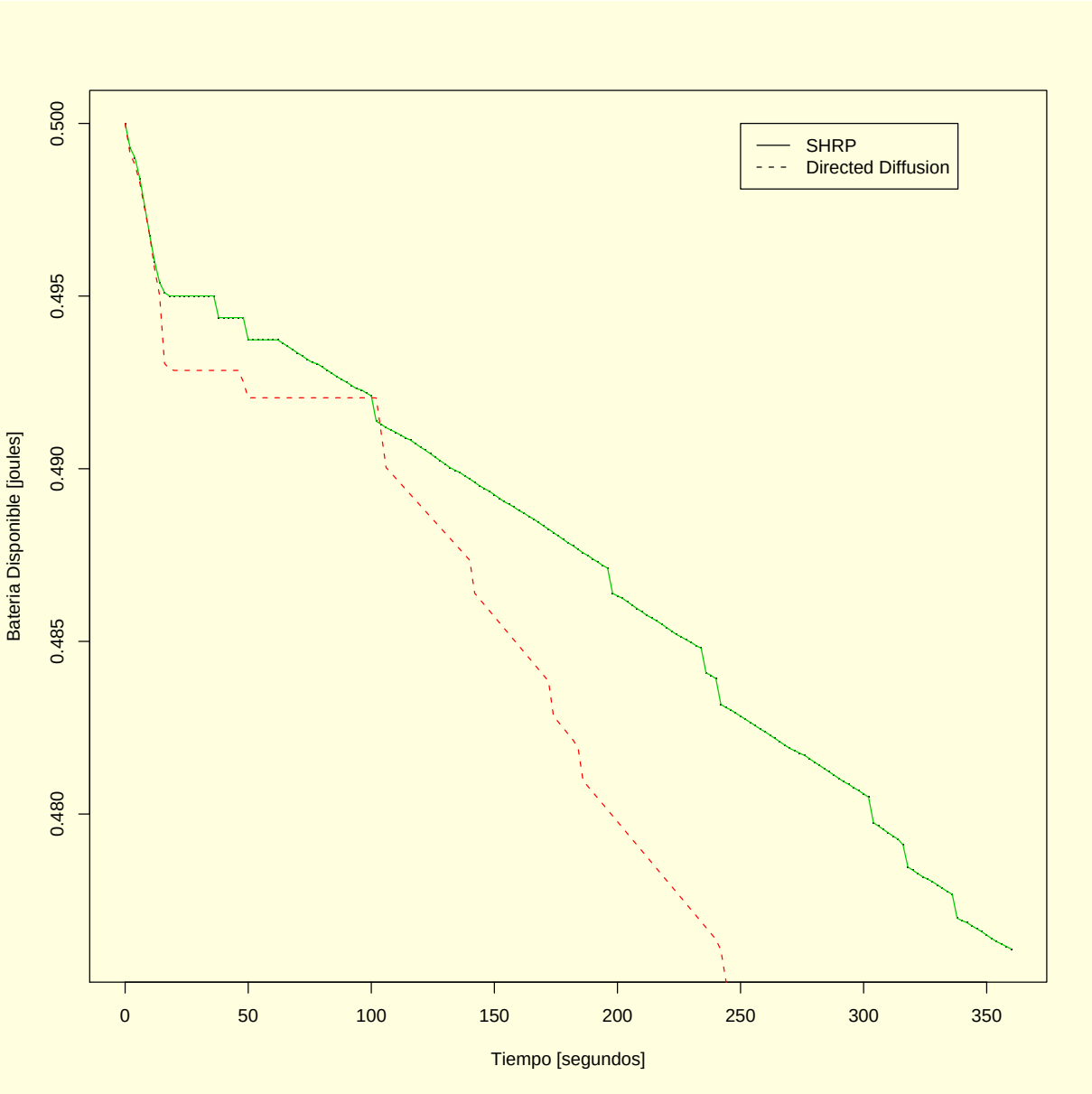

Figura 5.15: Comparación del consumo de bateria utilizando *SHRP* y *Directed Diffusion* para 100 nodos

entrega si para la aplicación no es lo más importante, ahorrando más energía y disminuyendo el retardo en la entrega.

- Por último y no menos importante, se ha mostrado experimentalmente que *SHRP* ofrece mayor confiabilidad en la entrega de mensajes en relación a *Directed Diffusion*, lo que es muy bueno, por ejemplo, para aplicaciones de monitoreo donde en situaciones críticas hay que tomar una decisión de control.

Capítulo 6

Conclusiones y Trabajo Futuro

En este capítulo se presentan las conclusiones alcanzadas luego del desarrollo de este trabajo.

En la sección 6.1 se presentan las conclusiones y finalmente, en la sección 6.2, se dan posibles extensiones para este trabajo.

6.1. Conclusiones

En este trabajo se ha propuesto un protocolo de encaminamiento para redes inalámbricas de sensores, llamado *SHRP*, que utiliza conjuntamente los valores de: la batería disponible, la calidad del enlace y el número de saltos hasta Sink para escoger la mejor ruta a utilizar con la finalidad de ofrecer confiabilidad en la entrega de mensajes y ahorro de energía. A pesar de que existen propuestas que manejan estas métricas por separado (aunque no necesariamente de la misma forma en que se presentó en este trabajo), no se encontró una propuesta que las combinara para obtener transmisiones más confiables.

El incremento en la confiabilidad viene dado al tomar en cuenta diversos factores presentes en las redes de sensores y asociados a las métricas de interés. Cada nodo no sólo posee información local, conoce también los peores valores de las métricas por cada camino que le ofrecen sus vecinos. Con estos valores puede tomar decisiones de encaminamiento que garantizan la llegada del mensaje al nodo Sink, sin necesidad de tener la información de cada uno de los nodos por los que pasará el mensaje, que por demás no es factible dado lo limitado de los recursos de memoria y procesamiento de los nodos sensores.

Las pruebas de simulación muestran el potencial del protocolo en cada uno de los criterios de evaluación estudiados: sobrecarga de mensajes de control, consumo de energía, confiabilidad de entrega de mensajes y tiempo de convergencia. El protocolo ofrece distintos parámetros para su configuración, por lo que se sugieren nuevos estudios que permitan determinar los parámetros ideales de acuerdo a la topología y la aplicación que se utilizará. Es posible disminuir la confiabilidad de entrega si para la aplicación no es lo más importante, ahorrando más energía y disminuyendo el retardo en la entrega.

6.2. Trabajo Futuro

Es posible ampliar el estudio experimental realizando comparaciones con otros protocolos. Existen propuestas bastante recientes que toman en cuenta la bateria del nodo con las cuales sería interesante comparar nuestra propuesta. El único inconveniente es que por lo general no esta disponible la implementación de dichos protocolos al tratarse de propuestas teóricas o de las que no se dispone código libre. A nivel de configuración

puede ser interesante determinar cuáles son los valores ideales para los parámetros de *SHRP* (i.e. cantidad y longitud de los rangos de energía, tamaño del paquete, timeout, etc) dependiendo de la aplicación y de la topología. Algunos experimentos adicionales también pueden realizarse para comprobar el comportamiento con otras topologías diferentes al tipo maya utilizada en este trabajo.

Sin embargo, la extensión más importante de este trabajo consiste en agregar el control de la potencia de transmisión de los nodos. Esto es factible dado que el protocolo maneja métricas de calidad de enlace como LQI y RSSI con lo que puede establecer umbrales de confianza en los que puede disminuir o aumentar la potencia para mantener la conectividad mientras ahorra energía.

Bibliografía

[1] Industrial Strength Wireless Accutech. http://www.adaptiveinstruments.com/downloads/collateral/industrial-strength-wireless.pdf. 2007.

[2] A Guide For the Clueless: IEEE 802.15.4 Standard for Low-Rate Wireless Personal Area Networks (LR-WPAN) A.D. Parker. http://lecs.cs.ucla.edu/ adparker/ee202a/hw2/. 2004.

[3] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci. Wireless sensor networks: a survey. *Computer Networks (Amsterdam, Netherlands: 1999)*, 38(4):393–422, 2002.

[4] J.Ñ. Al-Karaki and A. E. Kamal. Routing techniques in wireless sensor networks: a survey. *IEEE Wireless Communications*, 11(6):6–28, 2004.

[5] ZigBee Alliance. http://www.zigbee.org/en/about/.

[6] Argo Part of the Integrated Global Observation Strategy Argo Proyect. http://www-argo.ucsd.edu.

[7] C. Barenco, R. González, N. Cárdenas, and L.J. García-Villalba. A proposal of a wireless sensor network routing protocol. *Telecommunication Systems*, 38(1-2):61–68, 2008.

[8] Cambridge Advanced Learner Dictionary Cambridge University. http://dictionary.cambridge.org/define.asp?key5̄2014&dictc̄ald.

[9] N. Cardenas, C. Barenco, and L.J. García-Villalba. Using multiple route metrics in a sensor networks protocol. In *Proceeding of XXIII Simposium Nacional de la Unión Científica Internacional de Radio*, Madrid, Spain, September 2008.

[10] S. Chatterjea, S. di Luigi, and P. J. M. Havinga. Dirq: A directed query dissemination scheme for wireless sensor networks. In B. Kaminska, editor, *IASTED International Conference on Wireless Sensor Networks 2006, WSN 2006, Banff, Canada*, Wireless and Optical Communication, Calgary, July 2006. ACTA Press.

[11] Etienne C.R. de Oliveira and Célio V.N. de Albuquerque. Avaliação de protocolos de roteamento para redes ad hoc e rssf aplicados à tv digital interativa e cidades digitais. In *XXXIII Conferencia Latinoamericana de Informática (CLEI'2007)*, San Jose, Costa Rica, Octubre 2007.

[12] W. Heinzelman, J. Kulik, and H. Balakrishnan. In *Adaptive protocols for information dissemination in wireless sensor networks*, 1999.

[13] K. Holger and A. Willig. *Protocols and Architectures for Wireless Sensor Networks*. Wiley, 2005.

[14] C. Intanagonwiwat, R. Govindan, D. Estrin, J. Heidemann, and F. Silva. Directed diffusion for wireless sensor networks. In *IEEE/ACM Transactions on Networking*, pages 2–16. IEEE Computer Society, 2003.

[15] Helping Organizations Realize the Business Benefits of RFID Intel and Wireless SensorÑetwork Technologies. http://www.intel.com/cd/00/00/25/15/251558-251558.pdf. 2005.

[16] Instrumenting the World with Wireless SensorÑetworks Intel. http://research.cens.ucla.edu/pls/portal/url/item/f1746111b714d751e0306180528d2fce.

[17] Intel Fab Condition Based Maintenance Intel. http://www.intel.com/research/vert-manuf-condmaint.htm.

[18] Intel Mote Sensor Nets / RFID Intel. http://www.intel.com/research/ exploratory/motes.htm.

[19] Intel Motes Intel and Wireless Sensor Networks. http://www.intel.com/research/downloads/snoverviewcd.pdf. 2005.

[20] Inteligence Intel. http://www.intel.com/research/downloads/ intelligencenewsletter.pdf. 2004.

[21] Manufacturing/Energy Impact on Industry Intel and Society. http://www.intel.com/research/vert-manuf-condmaint.htm.

[22] The Promise of Wireless SensorÑetworks Intel. http://www.intel.com/pressroom/archive/backgrnd/ 20040316backgrounder.pdf, 2004.

[23] Vineyard Smart Agriculture Intel. http://www.intel.com/research/vert-agrivineyard.htm.

[24] Philo Juang, Hidekazu Oki, Yong Wang, Margaret Martonosi, Li S. Peh, and Daniel Rubenstein. Energy-efficient computing for wildlife tracking: design tradeoffs and early experiences with zebranet. In *Proceedings of the 10th international conference*

on Architectural support for programming languages and operating systems, volume 37, pages 96–107, New York, NY, USA, October 2002. ACM Press.

[25] Tracking vehicles with a UAV-delivered sensorñetwork k. Pister. http://robotics.eecs.berkeley.edu/pister/29palms0103/.

[26] T. Kevan. Shipboard machine monitoring for predictive maintenance. *sensors journal*, 23:s5–s8, October 2006.

[27] Alan Mainwaring, David Culler, Joseph Polastre, Robert Szewczyk, and John Anderson. Wireless sensor networks for habitat monitoring. In *WSNA '02: Proceedings of the 1st ACM international workshop on Wireless sensor networks and applications*, pages 88–97, New York, NY, USA, 2002. ACM.

[28] A. Manjeshwar and D. P. Agrawal. Teen: a routing protocol for enhanced efficiency in wireless sensor networks. In *Parallel and Distributed Processing Symposium., Proceedings 15th International*, pages 2009–2015, 2001.

[29] MannaSim. http://www.cpdee.ufmg.br/ manna/mannasim/index.htm.

[30] Kirk Martinez, Jane K. Hart, and Royan Ong. Environmental sensor networks. *Computer*, 37(8):50–56, 2004.

[31] Mason M. Medizade, John R. Ridgely, and Donald Nelson. Marginal expense oil well wireless surveillance meows - phase ii. Technical Report DE-FG26-02NT15293, Petrolects LLC, November 2004.

[32] Vivek Mhatre and Catherine Rosenberg. Design guidelines for wireless sensor networks: communication, clustering and aggregation. *Ad Hoc Networks*, 2(1):45–63, 2004.

[33] Masateru Minami, Shunsuke Saruwatari, Takuya Kashima, Takashi Morito, Hiroyuki Morikawa, and Tomonori Aoyama. Implementation-based approach for designing practical sensor network systems. In *APSEC '04: Proceedings of the 11th Asia-Pacific Software Engineering Conference (APSEC'04)*, pages 703–710, Washington, DC, USA, 2004. IEEE Computer Society.

[34] NS-2. http://www.isi.edu/nsnam/ns.

[35] MIT Object Tcl OTcl. http://otcl-tclcl.sourceforge.net/otcl.

[36] Jeongyeup Paek, K. Chintalapudi, R. Govindan, J. Caffrey, and S. Masri. A wireless sensor network for structural health monitoring: performance and experience. In *EmNets '05: Proceedings of the 2nd IEEE workshop on Embedded Networked Sensors*, pages 1–9, Washington, DC, USA, 2005. IEEE Computer Society.

[37] Joseph Polastre, Jason Hill, and David Culler. Versatile low power media access for wireless sensor networks. In *SenSys '04: Proceedings of the 2nd international conference on Embedded networked sensor systems*, pages 95–107, New York, NY, USA, 2004. ACM.

[38] Joseph Polastre, Jonathan Hui, Philip Levis, Jerry Zhao, David Culler, Scott Shenker, and Ion Stoica. A unifying link abstraction for wireless sensor networks. In *SenSys '05: Proceedings of the 3rd international conference on Embedded networked sensor systems*, pages 76–89, New York, NY, USA, 2005. ACM.

[39] Qualnet. http://www.scalable-networks.com/.

[40] Ruud Riem-vis. Cold chain management using an ultra low. power wireless sensor network. In *ACM/USENIX MobiSys 2004 International Workshop on Applications of Mobile Embedded Systems (WAMES 2004 online proceedings)*, Boston, USA, June 2004.

[41] Kay Römer and Friedemann Mattern. The design space of wireless sensor networks. *IEEE Wireless Communications*, 11(6):54–61, December 2004.

[42] Linnyer Beatrys Ruiz, Luiz Henrique A. Correia, Luiz Filipe M. Vieira, Daniel F. Macedo, Eduardo F. Nakamura, Carlos M. S. Figueiredo, Marcos Augusto M. Vieira, Eduardo Habib B. Maia, Daniel Camara, Antonio A. F. Loureiro, José Marcos S. Nogueira, Diógenes C. da Silva Jr., and Antônio O. Fernandes. Arquiteturas para redes de sensores sem fio. In *22 Simpósio Brasileiro de Redes de Computadores*, 2002.

[43] Sense. http://www.cs.rpi.edu/ cheng3/sense/.

[44] SensorSim. http://nesl.ee.ucla.edu/projects/sensorsim/.

[45] Victor Shnayder, Mark Hempstead, Bor rong Chen, Geoff Werner Allen, and Matt Welsh. Simulating the power consumption of large-scale sensor network applications. In *SenSys '04: Proceedings of the 2nd international conference on Embedded networked sensor systems*, pages 188–200, New York, NY, USA, 2004. ACM.

[46] Gyula Simon, Miklós Maróti, Ákos Lédeczi, György Balogh, Branislav Kusy, András Nádas, Gábor Pap, János Sallai, and Ken Frampton. Sensor network-based countersniper system. In *SenSys*, pages 1–12, 2004.

[47] Squalnet. http://nesl.ee.ucla.edu/project/show/23.

[48] K. Srinivasan and P. Levis. Rssi is under appreciated. In *Third Workshop on Embedded Sensor Networks Emnets 06*, Boston, MA, 2006.

[49] Claire Swedberg. Bp refinery uses rfid for evacuation system. *RFiD Journal*, 2006.

[50] CC2420 datasheet"Texas Instruments. http://www.chipcon.com/files/cc2420-data-sheet-1-4.pdf.

[51] T. Tokmouline, S. Madden, and I. Stoianov. Monitoring infrastructure using sensor networks. In *WSNA '02: Proceedings of the 1st ACM international workshop on Wireless sensor networks and applications*, New York, NY, USA, 2002. ACM.

[52] Truetime. http://www.control.lth.se/ dan/truetime/.

[53] Yu-Chee Tseng, Sze-Yao Ni, Yuh-Shyan Chen, and Jang-Ping Sheu. The broadcast storm problem in a mobile ad hoc network. *Wirel. Netw.*, 8(2/3):153–167, 2002.

[54] Vmnet. http://www.cs.ust.hk/vmnet/.

Apéndice A

La Tecnología IEEE 802.15.4

Una red inalámbrica de área personal con baja tasa de transmisión - llamada LR-WPAN (Low Rate - Wireless Personal Area Network) - es una red de comunicación simple que permite conectividad inalámbrica de aplicaciones con restricciones de energía y un ancho de banda relajado. El Grupo de Trabajo de Redes Inalámbricas de Área Personal IEEE 802.15.4, ha trabajado arduamente en la estandarización de las LP-WPAN. De hecho se ha establecido como el estándar de facto para las redes inalámbricas de sensores. La mayoría de los Motes disponibles en el mercado incorporan este estándar como mecanismo de comunicación.

A.1. Objetivos

Una LR-WPAN busca ser una red de fácil instalación que proporcione transferencia confiable de datos, muy bajo costo, razonable tiempo de vida de las baterías y corto rango de operación, mientras mantiene un protocolo simplificado y flexible.

Las principales metas del estándar son [2]:

- Muy Bajo consumo de potencia: En prácticamente cualquier dispositivo inalámbrico, el radio o componente de transmisión y recepción, es lo que más energía consume, incluso por encima del CPU y cualquier otro estado de activación de la tarjeta. Estos dispositivos conocidos como motes tienen grandes limitaciones de consumo eléctrico, al tener que operar en exteriores con una pequeña batería por períodos de meses o años.

- Muy Bajo costo de implementación: El costo final de los componentes que implementen una LP-WPAN debe ser muy pequeño, ya que por el tipo de aplicaciones al que se espera que apliquen, estas redes deben estar compuestas de numerosos dispositivos, tan baratos que incluso lleguen a ser considerados como desechables.

A.2. Componentes de una red IEEE-802.15.4

Dos tipos de dispositivos pueden participar en una red IEEE-802.15.4: Un disposivo que dispone todas las funcionalidades llamado FFD (Full-Function Device) y un dispositivo de funciones reducidas llamado RFD (Reduced-Function Device). El primero puede operar en la red en tres modos distintos, como coordinador de la red (PAN), coordinador o dispositivo. Un FFD puede hablar con RFD o con otros FFD, mientras que un RFD solo puede hablar con un FFD. Los RFD son interesantes en aplicaciones extremadamente simples, como un interruptor de luz o un sensor infrarrojo pasivo que no necesitan enviar grandes cantidades de datos y se asocian con un solo FFD a la vez.

Un sistema de acuerdo a este estándar requiere de por lo menos dos dispositivos donde uno de ellos debe ser FFD para que opere como coordinador PAN.

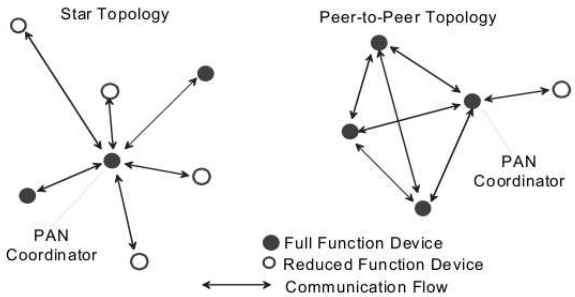

Figura A.1: Ejemplos de topologías estrella y peer-to-peer

A.3. Topologías de Red

Dependiendo de los requerimientos de la aplicación, una LR-WPAN puede operar utilizando una topología estrella o una topología peer-to-peer. Ambas son mostradas en la figura A.1.

En la topología estrella, la comunicación es establecida entre los dispositivos y un controlador central llamado coordinador PAN. En ambas topologías los nodos utilizan una dirección única de 64 bits. Sin embargo, una vez que el dispositivo se asocia puede negociar con el coordinador PAN una dirección corta de 16 bits.

La topología peer-to-peer también tiene un coordinador PAN, sin embargo, cualquier dispositivo puede comunicarse con otro siempre que este a su alcance. Esta topología permite implementar formaciones de red mucho más complejas. Utilizando múltiples saltos es posible que exista comunicación entre cualquier par de dispositivos de la red aún cuando no exista alcance de radio directo entre ellos.

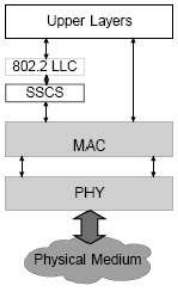

Figura A.2: Diagrama de las capas ofrecidas por IEEE-802.15.4

A.4. Arquitectura del estándar IEEE-802.15.4

Para simplificar el estándar se ha definido en capas (ver figura A.2) de forma similar a la estructura del modelo OSI (Open Systems Interconnection) donde cada capa es responsable de una parte del estándar y ofrece servicios a las capas superiores.

Un dispositivo LR-WPAN está compuesto por una capa física (PHY) que controla a bajo nivel la transmisión de radio frecuencia (RF) y una capa MAC que provee acceso al canal físico para todos los tipos de transferencia.

Existe una propuesta adicional al estandár realizada por ZigBee Alliance, organización conformada por un grupo de empresas, en la cual incorporan una especificación para las capas de red (NWK) y de aplicación (APL) basadas en el estándar IEEE-802.15.4 y que sólo es disponible para sus miembros. Su objetivo de ofrecer soluciones ínteroperables en el área de las redes de sensores [5].

Capa Física (PHY) La especificación IEEE802.15.4 indica que esta capa debe cumplir con las siguientes funciones:

- Activación y Desactivación de nodos

- Detección de energía
- Indicador de calidad del enlace
- Detección de actividad del canal
- Recepción y Transmisión de datos

Ofrece la capacidad de operar en tres bandas de frecuencias libres, no sujetas a las regulaciones y reservación explícita de los canales:

- 868 MHz (banda libre Europea), lo que permite un canal de 20 Kbps.
- 902-928 MHz que por ser más ancha (26 MHz) permite 10 canales de 40 Kbps.
- 2.4-2.48 GHz con la posibilidad de ofrecer 16 canales de 250 Kbps.

Las distancias posibles pueden llegar hasta 300 mts pero, por el bien conocido fenómeno de aumento exponencial de la potencia con respecto a la distancia, el consumo de energía sería enorme. Así que, mientras más corta sea la distancia entre los dispositivos, menor será el consumo de energía, en las transmisiones de información.

En la banda de 2.4 GHz se modula el canal con O-QPSK, el cual define una constelación de 4 fases (45, 135, 225 y 315 grados) por lo que se transmite en el enlace de última milla a dos bits por baudio. La banda de 868 MHz se modula con BPSK. En ambos casos transforma los bits que circulan por el canal en chips o secuencias de 0 y 1. Los chips son definidos pseudo-aleatoriamente de mutuo acuerdo entre el emisor y el receptor. En términos sencillos, el emisor multiplica la señal recibida por el chip, envía la señal, y luego el receptor extrae de la portadora el mismo chip y al hacerlo, puede recuperar la información codificada, descartando al resto de las señales presentes en el canal.

A.4.1. Capa de Acceso al Medio (MAC)

Esta capa, también definida en IEEE802.15.4, asegura el control de las conexiones punto a punto entre nodos para brindar confiabilidad a la transferencia de datos. Las funciones que debe realizar son:

- Transmisión de la trama de sondeo o baliza
- Sincronización de la trama baliza dentro de la supertrama
- Asociación y des-asociación de nodos
- CDMA/CA a dos vías (sin CTS ni RTS)
- Transmisión en períodos de contención (CAP) y garantizado (GTS)

Mediante el uso de una supertrama que es enviada por el coordinador, es posible lograr multiplexar la comunicación de todos los tipos de nodos presentes en la red. Esta funciona por multiplexación de tiempo, con 16 ranuras del mismo tanaño, para que los nodos coloquen sus datos en el medio de transmisión.

La supertrama está dividida en 4 períodos de tiempo como se puede observar en la figura A.3:

- Período de contención (CAP)
- Ranuras de tiempo garantizadas (GTS)
- Ranura de la trama baliza
- Período de inactividad o bloqueo

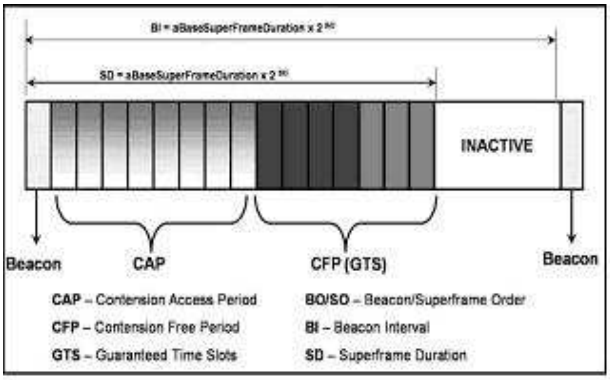

Figura A.3: Supertrama de sincronización por tiempo en la capa MAC

En el período de contención los nodos se disputan el uso de alguna de las ranuras usando CSMA-CA y pueden haber colisiones. En cambio en GTS la conexión está asegurada pues son ranuras que se reservan de antemano. Todo esto se negocia a través de la trama baliza (Beacon Frame). Durante el período de bloqueo o inactividad todos los nodos, hasta el coordinador, duermen para ahorrar energía. Estos intervalos pueden ir desde 15 mseg. hasta 4 min.

Apéndice B

Redes Inalámbricas de Sensores

Una conexión íntima entre los sensores y el ambiente donde se encuentra, le permite a los sensores proveer información localizada que sería díficil de obtener a través de la instrumentación tradicional. La integración de procesamiento local y almacenamiento, le permite a los nodos sensores realizar complejos procesos de filtraje, algoritmos de compresión y ejecutar funciones específicas de la aplicación. La habilidad de comunicarse les permite además cooperar entre si en la ejecución de tareas más complejas, tales como muestreo estadístico, agregación de datos y control del estado del sistema.

Las redes de sensores son construidas con componentes de bajo costo que son favorecidas por la ley de Moore, en cuanto a la reducción del tamaño y del costo. Llegará el día en que el tamaño de los nodos sea como una partícula de polvo y sólo cueste unos centavos. En la actualidad, radios de bajo consumo de energía y el uso de pilas de protocolos, permiten generalizar las comunicaciones en lugar de usar telemetría punto a punto. Las habilidades de cómputo y de red le permiten a las redes de sensores ser reprogramadas en el campo, luego de su despliegue. Los nodos tienen la habilidad de adaptar su operación en el tiempo respondiendo a los cambios ambientales y a la

condición de la red como tal.

En la sección B.1 se describen las características que están presentes comúnmente en las redes de sensores, en B.2 se enumeran las funcionalidades de las redes de sensores. Luego, en B.3 se presenta la clasificación de las aplicaciones de las redes de sensores. Luego, en la sección B.3.5 se describen los fundamentos de las redes centradas en los datos. Finalmente en B.4 se muestran las métricas de evaluación para las redes de sensores.

B.1. Características comunes de las Redes Inalámbricas de Sensores (RIS)

Entre las características más importantes que podemos encontrar en cualquier red de sensores, tenemos:

- Están compuestas por un gran número de nodos, pudiendo llegar al orden de los miles (hasta 65.536, por restricciones de direccionamiento).
- Muestran un flujo asimétrico de datos, desde los nodos de captura de datos (sensor node) a una estación base.
- Las comunicaciones son originadas por consultas o eventos.
- En cada nodo existe una cantidad limitada de energía al ser alimentados por baterías, que en muchas aplicaciones es imposible de reemplazar o recargar ya que por ejemplo, pudieron ser esparcidos desde un avión en un terreno de difícil acceso.

- Los nodos están propensos a fallar por distintas razones y esto debe ser tolerado por el sistema.
- Se emplean principalmente las comunicaciones de difusión (Broadcast) en lugar de las comunicaciones punto a punto.
- Los nodos no poseen un identificador único universal, tal como lo es un número IP.
- La seguridad, tanto física como a nivel de la comunicación, es más limitada que en los enfoques de redes inalámbricas convencionales, como en WiFi.

B.2. Modelo Funcional para las Redes de Sensores

Las principales funcionalidades de las redes de sensores pueden separarse en cinco grupos de actividades [42]: establecimiento de la red, administración, monitoreo, procesamiento y comunicación. Estas fases pueden realizarse de forma simultánea y pueden estar activas en distintos momentos del tiempo de vida de las redes de sensores. A continuación se describen:

- Establecimiento de la red: En este grupo se incluyen tareas como: difinición del área de cobertura, distribución de los nodos, conectividad, topología, dimensionamiento, tipos de sensores a utilizar, políticas para despertar a los nodos, organización, etc.
- Administración: Manejo y corrección de las situaciones anormales causadas por fallos en los nodos, adaptación a las condiciones de energía de la red, llegada de

nuevos nodos, etc.

- Monitoreo: Configuración de la frecuencia y tiempo de exposición del sensor a su objetivo de medición (frecuencia del muestreo), tipos de datos, ancho de banda y frecuencia de actualización.
- Comunicación: Establecer el medio de acceso (WLAN, Bluetooth, ZigBee), manejar la topología de la red, consideraciones sobre la movilidad de los nodos en caso que exista.
- Procesamiento: algoritmos de control, compresión, seguridad, encriptación, codificación y corrección de errores.

B.3. Clasificación de las Aplicaciones para Redes de Sensores

Las aplicaciones en Redes de Sensores pueden ser clasificadas en: (i) Monitoreo y Control (ii) Seguridad (iii) Seguimiento o rastreo o (iv) híbridas

B.3.1. Monitoreo y Control

Las aplicaciones de este tipo por lo general utilizan protocolos de encaminamiento basados en árbol, donde cada árbol tiene como raíz una estación base con más alta capacidad de recursos. Los nodos con mayor cantidad de descendientes transmiten más datos, así que pueden ser puntos de embotellamiento de energía. Normalmente necesitan bajas tasas de datos y tiempo de vida extremamente largos.

Una vez la red es desplegada, los nodos deben descubrir la topología de la red y estimar una estrategia óptima de encaminamiento. Algunas implementaciones aprovechan que la topología física de red es relativamente constante para calcular la topología óptima de la red externamente y solo comunicarle a los nodos la información de encaminamiento que deben seguir.

Los intervalos típicos para el envío de mensajes periódicas es de 1 a 15 minutos y los parámetros medidos comunmente son: temperatura, intensidad de luz y humedad, que son parámetros que no cambian rápidamente y tienen bajas tasas de medición.

Dentro de este rubro se encuentran las aplicaciones que se encargan de la recolección de datos de ambientes de interés que típicamente usan intervalos de medidas y no tienen restricciones estrictas de latencia. En general, los datos son recolectados para futuros análisis.

Los nodos sensores estarán en un modo de ahorro de energía la mayor parte de su tiempo; sólo serán despertados al momento de enviar y recibir datos. Eventualmente, los nodos fallarán por falta de energía, y el proceso de reconfiguración llevará a un gasto extra de energía de los nodos restantes. Sin embargo, no es un evento que suceda muy frecuentemente.

Los principales requerimientos de los sistemas de monitoreo de ambiente son: largo tiempo de vida; bajas tasas de datos y topologías estáticas.

B.3.2. Seguridad

El segundo tipo de aplicaciones en Redes de Sensores son los sistemas de monitoreo de seguridad. Están compuestos por nodos que se quedan en lugares fijos de un ambiente y que están contínuamente monitoreando uno o más sensores para la detección de anomalías. Es un sistema distinto del monitoreo de datos ambientales ya que frecuentemente tiene que verificar el estatus de los sensores pero sólo transmite datos cuando haya una violación de seguridad.

En un árbol de recolección de datos, cada nodo debe transmitir su dato a sus descendientes, así que un árbol óptimo es un árbol pequeño y largo. En contrapartida, en una red de seguridad la configuración óptima tendrá una topología lineal, formando un ciclo Hamiltoniano de la red. El consumo de energía es proporcional al número de nodos descendientes. En una red lineal, cada nodo tiene sólo un descendiente. Así que el consumo de energía será distribuido a lo largo de la red.

Las normas aceptables de sistemas de seguridad actuales son que cada sensor debe chequear aproximadamente cada hora.

En sistemas de seguridad reducir la latencia de las alarmas es mucho más importante que reducir la energía consumida en las transmisiones. Sin embargo, las violaciones de seguridad o los eventos de alarma deben ser esporádicos.

Otra consideración importante que involucra un mayor consumo de energía es la necesidad que los nodos confirmen que sus vecinos están funcionando y que asegure que están siempre preparados para instantáneamente enviar alarmas.

B.3.3. Seguimiento o Rastreo

Un tercer escenario discutido en Redes de Sensores es el rastreo de objetos dentro de un espacio determinado. En sistemas de rastreo como los utilizados por UPS (United Parcel Service) los objetos deben pasar por puntos de chequeo, pero no siempre se puede garantizar que el objeto pasará a través de esos puntos.

Con las Redes de Sensores, los objetos pueden ser sencillamente rastreados a través de sensores. Los nodos en ese escenario pueden ser etiquetas activas que anuncian la presencia de un dispositivo. Así que es posible preguntar a un objeto no sólo cuando fue la última vez que fue rastreado, también donde se encuentra actualmente.

De manera distinta a las redes de seguridad, las aplicaciones de rastreo presentan un cambio contínuo de topología ya que los nodos están en movimiento. De manera ideal, el sistema debería, automáticamente, configurarse a cualquier posición física. Sin embargo, en la realidad los nodos tienen restricciones sobre sus posibles posiciones y la red de sensores debe ser capaz de dar una respuesta en caso que esa restricción sea violada. La red debe indicar cualquier problema potencial como descubrir nuevos enlaces y determinar la calidad de los enlaces.

B.3.4. Redes Híbridas

Existen escenarios de aplicaciones que poseen aspectos de todas las categorías mencionadas anteriormente. En estos casos se requiere una arquitectura que contemple características descritas en distintas categorías previamente comentadas.

B.3.5. Redes Centradas en los Datos

Un usuario de una red de sensores inalámbricos desea saber algo sobre el ambiente físico que interactua con la red y por lo general no le importa el nodo sensor que realiza la medición. Por ejemplo, un usuario necesita "la temperatura promedio en la habitación C-1 del edificio X."en lugar de ."obtener los valores de la temperatura de los nodos sensores 13,47,2225 14592 y 14593 y promediarlos". Es preferible ofrecerle a los usuarios el nombre del dato en el que están interesados y no el (o conjunto de) nodo(s) que producen los datos.

En una red tradicional basada en IP, este requerimiento implica la introducción de un sistema de nombres sobre las direcciones IP y de un servicio similar a DNS que provea la traducción de los nombres (con significado para el usuario) a las direcciones IP (con significado para el protocolo de encaminamiento). En las redes de sensores, sin embargo, estos niveles de direccionamiento pueden ser eliminados y los atributos de los usuarios pueden ser usados directamente para encontrar grupos de nodos. Este concepto es conocido como direccionamiento centrado en los datos o basado en el contenido, y permite que los datos de la aplicación tengan significado dentro de la operación de la red (especialmente para los protocolos de encaminamiento). Además, permite incorporar técnicas de procesamiento dentro de la red.

B.4. Métricas de Evaluación de las Redes de Sensores

Las métricas más importantes en las Redes de Sensores son: tiempo de vida, cobertura, costo, facilidad de despliegue, tiempo de respuesta, precisión temporal, seguridad

y tasa de muestreo efectiva.

Estas métricas están interrelacionadas y permiten definir las plataformas a utilizar así como las necesidades de las aplicaciones. La plataforma de un sistema puede atender de manera satisfactoria a una aplicación si y sólo si sus capacidades cumplen con las necesidades de dicha aplicación.

A continuación se describen cada una de las métricas:

B.4.1. Costo y facilidad de despliegue

Una de las grandes ventajas de las Redes de Sensores es la facilidad de despliegue. Para que el despliegue sea satisfactorio, la red de sensores debe ser configurada automáticamente. Los nodos podrían ser ubicados por personas no entrenadas y dejar que el sistema funcione de manera sencilla.

A lo largo del tiempo de vida de la Red de Sensores se pueden generar interferencias en las comunicaciones entre los nodos, ya sea porque los nodos sean reubicados o por la incorporación de nuevos objetos físicos en el ambiente. La red debe, automáticamente, reconfigurarse para tolerar esos tipos de ocurrencias.

Cuando sea necesario, la Red de Sensores puede generar requisiciones para su mantenimiento. Eso significa que en un despliegue real, una parte de la energía debe estar dedicada a manutención y verificación del sistema.

B.4.2. Cobertura

Es una ventaja tener la posibilidad de desplegar una red de sensores en una gran área de cobertura física. Eso puede significar un incremento en el valor del sistema al usuario final.

El uso de técnicas de comunicación de múltiples saltos puede extender la cobertura de la red, más allá del alcance de transmisión. En teoría, podríamos extender la red de manera infinita. Sin embargo, los protocolos de múltiples saltos aumentan el consumo de energía de los nodos, lo que disminuye el tiempo de vida de la red. Adicionalmente se necesita un mínimo de densidad de los nodos, lo que aumenta el costo de despliegue.

La escalabilidad es un componente importante en las Redes de Sensores. Un usuario puede desplegar una red pequeña y luego agregar nuevos puntos de captura de datos. A medida que más puntos de observación sean agregados, mayor será la cantidad de datos transmitidos, lo que aumentará el consumo de energía.

B.4.3. Tiempo de Vida

El factor principal del tiempo de vida de una Red de Sensores es su capacidad de energía. Cada nodo debe ser capaz de gestionar su energía local para maximizar su tiempo de vida. Por ejemplo, en un sistema de seguridad, cada nodo debe sobrevivir el mayor tiempo posible ya que, por su topología, una única falla crea una vulnerabilidad en el sistema de seguridad.

El factor más significativo en el tiempo de vida es el consumo de potencia de radio. A través de la disminución de la potencia de salida o del ciclo de ocupación de la

radio podemos reducir el consumo por concepto de transmisión. Ambas alternativas sacrifican otras métricas.

B.4.4. Tasa de Muestreo Efectiva

En un sistema de recolección de datos, la tasa de muestreo es la métrica más importante. La tasa de muestreo efectiva se define como la tasa en la cual el sensor mide alguna variable y envía la información a un punto central.

Afortunadamente, la recolección de datos necesita tasas de muestreo bastante bajas. Además de la tasa de muestreo del sensor hay que considerar el impacto de las arquitecturas de red de múltiples saltos, necesarias para efectivamente enviar los datos de los nodos.

Uno de los mecanismos usados para aumentar la tasa de muestreo efectiva es el uso de la capacidad de procesamiento dentro de la red. Varias formas de compresión espacial y temporal consisten en reducir el ancho de banda de comunicación mientras se mantiene la misma tasa efectiva de muestreo. Además, el almacenamiento local puede ser usado para recolectar y almacenar datos con una alta tasa por pequeños períodos de tiempo. El procesamiento dentro de la red puede ser usado para determinar si un evento interesante ocurrió y automáticamente activar el almacenamiento del dato. Después, ese dato puede ser transmitido. Si no hay procesamiento local, las lecturas redundantes de los sensores deben ser transmitidas.

B.4.5. Precisión temporal

La precisión temporal depende del entorno de monitoreo. Por ejemplo, si se quiere la temperatura media de un edificio, los muestreos deben ser correlacionados en unidades de segundos. Entretanto, para determinar si un edificio reacciona a un evento sísmico, se necesita una precisión de milisegundos.

Para alcanzar la precisión temporal, la red debe ser capaz de construir y mantener una base de tiempo global que puede ser usada para ordenar cronológicamente muestreos y eventos. En un sistema distribuido, se requiere de un consumo extra para mantener la sincronización del reloj. La información de sincronismo de reloj debe ser continuamente comunicada a través de los nodos. La frecuencia de los mensajes es dependiente de la precisión de reloj deseada.

B.4.6. Tiempo de Respuesta

Particularmente, en sistemas de alarmas, el tiempo de respuesta es una métrica muy importante. Independiente de la operación de gestión de energía, los nodos deben ser capaces de tener alta prioridad de comunicación en la red. Aunque esos eventos son esporádicos, pueden ocurrir sin avisos.

El tiempo de respuesta también es importante en entornos de monitoreo de ambientes, por ejemplo cuando se tiene máquinas y equipos de control de fábrica.

El tiempo de respuesta puede ser mejorado a través de la inclusión de nodos que estén conectados a energía todo el tiempo. Esos nodos pueden escuchar los mensajes de

alarma y reenviarlos a través de una ruta determinada que garantice tanto la eficiencia como la rapidez. Este tipo de soluciones reduce la facilidad de despliegue.

B.4.7. Seguridad

Las Redes de Sensores deben mantener las informaciones recolectadas de manera segura. No sólo se trata de mantener la privacidad sino también de autenticar los datos. Por ejemplo, es posible generar una falsa alarma o reenviar una alarma antigua como si fuera reciente. También se debe evitar la interferencia de señales.

Apéndice C

Herramientas de Simulación para Redes inalámbricas de Sensores

A la hora de escoger la herramienta de simulación para el proyecto, es necesario tomar en cuenta el ambiente, dispositivos y tecnologías que serán utilizados, de forma tal, que los escenarios creados por la herramienta de simulación sean los más cercanos a la realidad. Para este caso de estudio se debe considerar:

- Los equipos a utilizar son motes Mica y Telos
- La tecnología que utilizan dichos dispositivos es el estandar IEEE-802.15.4
- Los motes son programados utilizando el lenguaje NesC.

En función a estas características se definen los parámetros de evaluación que se utilizarán para escoger la herramienta de simulación:

- Soporte a tecnología de redes inalámbricas IEEE 802.15.4.

- Posibilidad de programación en NesC para aprovechar código a la hora de implementar el protocolo Simulación de Redes y no sólo del hardware de los sensores.
- Posibilidad de simulación de Motes tanto como Mica2, MicaZ y Telos B.
- Poseer modelo de simulación de gasto de energía.
- Ser de código abierto y libre.

A continuación se describen cada una de las herramientas estudiadas:

C.1. Sensorsim [44]

Es un framework de simulación para la creación de modelos de simulación de Redes Inalámbricas de Sensores. Se ejecuta a partir de la herramienta de simulación de redes llamada NS-2 [34].

Posee las siguientes características:

- Permite la creación de Modelos de sensores.
- Soporta pilas de protocolos ligeras para redes inalámbricas de microsensores
- Permite la generación de escenarios de simulación, antes de arrancar la simulación.
- Soporta simulación híbrida (simulación y emulación).

Comentarios:

Parece ser una herramienta interesante ya que se basa en el entorno de simulación NS-2, muy usado por la comunidad académica. Sin embargo, es un framework que ya no es soportado por el grupo que lo desarrolló, así que sus códigos de programas no se encuentran disponibles públicamente. También su desarrollo es en lenguajes C++ y Otcl, lo que hace que los programas de simulación no puedan ser aprovechados directamente para ser instalados en los Motes. Hace simulaciones no sólo del hardware, sino también del software.

C.2. Squalnet [47]

Squalnet es una extensión de la herramienta Qualnet [39]. Su unidad de simulación es un nodo que posee dos pilas de protocolos, una TCP/IP y otra no TCP/IP; lo que permite la simulación de otras arquitecturas de red que no sean IP. Permite la utilización de programas escritos en NesC, para la simulación de la capa de aplicación.

Con esta herramienta podemos simular:

- Sensores de temperatura y posicionamiento.
- Modelos de baterías.
- Modelos de consumo de energía de los procesadores.
- Modelo específico de tráfico para redes de sensores.
- Adicionalmente da soporte a las siguientes características

- Pilas de protocolos no TCP/IP.
- Protocolo S-MAC, una capa MAC especial para redes de sensores.
- Modelos de difusión de tráfico (encaminamiento) del TinyOS.

Comentarios:

La herramienta parece bastante completa, pero tiene la desventaja de que necesita el entorno de simulación Qualnet, que no es libre.

C.3. SENSE [43]

La herramienta SENSE posee las siguientes características:

- Extensibilidad: modelo basado en componentes.
- Reusabilidad: templates en C++.
- Escalabilidad: ejecución de componentes paralelos que sean compatibles.

Con esta herramienta podemos simular:

- Modelo de batería: batería lineal, Tasa Dependiente de Descarga y Relaxation Battery.
- Capa de Aplicación: Vecinos aleatorios, CBR (Constant Bit Error).

- Capa de Red: Flooding Simple, Versión simplificada del protocolo de encaminamiento AODV (sin reparación de rutas), una versión simplificada del protocolo DSR (sin reparación de rutas).
- Capa MAC: Nullmac, IEEE 802.11 con DCF;
- Capa física: Transceptores Duplex, Canales Wireless;
- Máquina de Simulación: Costsimeng (secuencial)

Comentarios:

La herramienta incluye varias funcionalidades que pueden ser bien útiles, pero tiene la desventaja de que los códigos fuentes de simulación deben ser escritos en C++, por lo que no es posible aprovechar el código para instalarlo directamente en los motes que se disponen. Además de eso, parece no soportar el estándar IEEE 802.15.4 por lo que requeriría simular todo el standard

C.4. Mannasim [29]

Es una herramienta de simulación de Redes de Sensores que posee dos partes:

- Mannasim Framework: Mannasim es un framework de simulación para WSN basado en la herramienta NS-2 [24]. El Mannasim extiende el NS-2 con módulos para el diseño, desarrollo y análisis de aplicaciones WSN.

- Herramienta generadora de Scripts de simulación: El SGT (Script Generator Tool) es un frontend de scripts de simulación TCL. Está escrito en Java, así que, es independiente de la plataforma.

El objetivo del Mannasim es crear un entorno detallado de simulación de distintos nodos de sensores y aplicaciones, para análisis de algoritmos y aplicaciones.

Con esta herramienta podemos simular:

- Capa MAC IEEE 802.11.
- Motes Crossbow Mica2.
- Antenas apropiadas para motes mica2 (máximo 1.5 metro de altura).
- Diversos modelos de propagación de radio: Freespace, Shadowing, Shadowing-vis, Tworayground.
- El punto de acceso a otra red (AP).

Comentarios:

Es una herramienta con varios características para la simulación de WSN ya que usa el NS-2 como base, y así permite que simulemos protocolos en otras capas que no sean sólo las capas física y de enlace, además de permitir simular la conexión de una WSN a otra red, a través de un punto de acceso. La desventaja es que no simula el estándar IEEE 802.15.4 sólo IEEE 802.11.

C.5. Vmnet [54]

En Vmnet, un nodo WSN es emulado como una VMN (Virtual Mote Network). El CPU de un mote (nodo sensor) es emulado en ciclos de reloj. La unidad de sensibilidad y otros hardware periféricos también son emulados con muchos detalles. La señal de radio es emulada a través de la comunicación entre VMs con efectos de pérdida de señal y ruido. Además, Vmnet recoge valores de parámetros del mundo real y guarda estados detallados del código en la aplicación. Como resultado, o código binario de la aplicación Vmnet puede ser ejecutado directamente en el Vm, y el desempeño de la aplicación, como tiempo de respuesta y consumo de energía, puede ser reportado en la Vmnet.

El Vmnet posee una arquitectura de módulos que permite el ensamblado de componentes de hardware virtuales. Actualmente emula el mote mica2 de Crossbow. El módulo de CPU virtual es el Atmel usado en los mica2. Así que, aplicaciones TinyOS y TinyDB pueden ser evaluadas en una Vmnet. Posee también herramientas sencillas para configuración e implantación de Vmn.

Comentarios:

Es una herramienta que tiene la ventaja que puede aprovechar los códigos fuentes desarrollados en la simulación para ejecutarlos en los motes, siempre que sean mica2. La desventaja es que en la parte de simulación de red no está claro como podemos simular una verdadera red IEEE 802.15.4, ya que se usa la emulación Ethernet como transporte de las señales entre los nodos simulados.

C.6. Truetime [52]

Es un simulador basado en Matlab/Simulink para el control de sistemas en tiempo real. Escrito en C++ y basado en eventos.

Con esta herramienta podemos simular:

- Recepción de interrupciones externas.
- Permite hacer llamadas a diagramas de bloques de Simulink.
- Posee soporte a módulos de red (Ethernet, CAN, TDMA, Round Robin y ethernet conmutada).
- Soporta tanto 802.11b como 802.15.4.
- Dispositivos que utilizan baterías

Comentarios:

No es un simulador específico para Redes de Sensores, así que tendríamos que abstraer algunas funcionalidades de un Mote. La principal desventaja es que necesita la utilización de Matlab, que es un software propietario.

C.7. PowerTOSSIM

Es un ambiente de simulación escalable para redes inalámbricas de Sensores que provee una estimación precisa del consumo de potencia por nodo [45].

PowerTOSSIM es una extensión de TOSSIM que más que un ambiente de simulación es un emulador orientado a eventos para aplicaciones de TinyOS. Esta herramienta permite que un programa escrito en NesC sea ejecutado directamente en un PC mostrando el mismo funcionamiento que debería tener en un Mote.

En PowerTOSSIM cada uno de los componentes de TinyOS asociado a un dispositivo, tales como: el radio, eeprom, leds, etc, son instrumentados para obtener una traza de la actividad de cada dispositivo. Luego dicha traza es analizada para determinar cuántos eventos ocurrieron durante la ejecución del programa y que gasto de energía está asociado a cada uno de ellos, a partir de esto se puede calcular el consumo de potencia en cada nodo que ejecuta el programa.

Posee modelos del consumo de energía para los Motes Mica2 de Crossbow. Las pruebas realizadas indican que se pueden alcanzar aproximaciones bastante precisas del consumo de energía con un nivel de error inferior al 14 % respecto al consumo real de cada Mote al ejecutar un programa.

Comentarios:

Permite evaluar directamente el consumo de energía de programas en NesC, sin que sea necesario elaborar modelos del comportamiento de los mismos, lo cual es una ventaja importante, adicionalmente el PowerTOSSIM viene incluido en las versiones más recientes del TinyOS por lo que es muy sencillo de obtener, sin embargo, al parecer sólo cuenta con modelos para los componentes específicos del mote Mica2, como el microcontrolador (el Atmel ATmega128) y el chip de radio (Chipcon CC1100).

Sería necesario hacer un esfuerzo para agregar o configurar modelos de otros microcontroladores, chips de radio y sensores para poder modelar el comportamiento de otros motes. La información más reciente de la herramienta en su Web site original se remonta al 2004, por lo que pareciera que no se ha continuado con su desarrollo.