ESCUELA POLITÉCNICA DEL EJÉRCITO

DEPARTAMENTO DE ELÉCTRICA Y ELECTRÓNICA

CARRERA DE INGENIERÍA EN ELECTRÓNICA Y TELECOMUNICACIONES

PROYECTO DE GRADO PARA LA OBTENCIÓN DEL TÍTULO DE INGENIERÍA

Análisis del desempeño de una red WPAN Basado en el estándar IEEE 802.15.4 utilizando Network Simulator 2

Santiago Xavier Villacrés Torres

SANGOLQUÍ – ECUADOR

2009

CERTIFICACIÓN

Certificamos que el presente proyecto de grado titulado: “ANÁLISIS DEL DESEMPEÑO DE UNA RED WPAN BASADO EN EL ESTÁNDAR IEEE 802.15.4 UTILIZANDO NETWORK SIMULATOR 2”, ha sido desarrollado en su totalidad por el señor SANTIAGO XAVIER VILLACRÈS TORRES con CC: 1719006650, bajo nuestra dirección.

Atentamente

Ing. Román Lara	Ing. Gonzalo Olmedo
DIRECTOR	**CODIRECTOR**

RESUMEN

El presente documento trata sobre el análisis del desempeño de una red de área personal basada en la utilización del estándar IEEE 802.15.4

Se realizó varios escenarios de pruebas en los cuales se simulaba el envío de datos entre los nodos pertenecientes a la red.

En total se crearan quince simulaciones a las cuales se les variaba la densidad de nodos y el modelo de propagación, manteniendo fijo el protocolo de enrutamiento, siendo AODV el escogido.

El área en la cual se simulaba cada escenario de red cubría una superficie de 60x60 m^2, y la densidad de nodos fijos era de 10, 17, 20, 40 y 50 nodos respectivamente. A cada escenario se le alternaba el modelo de propagación, siendo estos Dos Rayos, Free Space y Shadowing

El programa usado par realizara las simulaciones fue Network Simulator versión 2.32, y la aplicación para interpretar y analizar los resultados fue Trace Graph versión 1, el cual permite obtener todos los parámetros necesarios para realizar el respectivo análisis.

Con los parámetros obtenidos de cada escenario simulado se elaboraron comparaciones entre ellos y su realizó el análisis del desempeño de una WPAN.

DEDICATORIA

Este proyecto de grado está dedicado a toda mi familia y en especial a mis padres, Patricio y Marcia; cuyo esfuerzo y apoyo hicieron posible que pueda culminar esta fase universitaria.

AGRADECIMIENTO

Agradezco a mi familia por brindarme el apoyo que necesitaba en los momentos precisos, por enseñarme que la responsabilidad es la cualidad más importante de una persona y por darme la fortaleza y respaldo total para cumplir con mis metas.

También agradezco a mi Director y Codirector de Tesis, quienes siempre estuvieron dispuestos a guiarme cuando necesitaba ayuda en la elaboración del presente proyecto de grado

A mis amigos de igual forma también les agradezco por compartir conmigo estos años de estudios, ya que la colaboración mutua de todos nos ha llevado a finalizar con éxito esta carrera y nos ha dejado gratos recuerdos.

PRÓLOGO

En la actualidad el estándar IEEE 802.15.4, conocido de manera general como ZigBee, ha permitido la evolución de prestaciones en redes inalámbricas de área personal (WPAN), gracias a que los dispositivos desarrollados para su uso, presentan poco requerimiento de ancho de banda y bajo consumo de energía.

Por lo que ante el creciente uso de ZigBee, es de gran importancia conocer cual es su desempeño dentro de una WPAN, para saber cuales son sus aspectos favorables y desfavorables al momento de transmitir paquetes, todo esto mediante el uso del simulador “Network Simulator 2 (NS-2)”, que facilita la creación de escenarios en los cuales se puede modificar los modelos de propagación o los protocolos de encaminamiento.

Además, el presente proyecto de grado dará continuidad a anteriores estudios de desempeño de redes inalámbricas realizados en la ESPE, que estaban basados principalmente en el estándar IEEE 802.11

En los primeros capítulos del presente proyecto se describe toda la parte teórica referente al estándar IEEE 802.15.4 y al Grupo ZigBee Alliance, dentro de lo cual constan las características generales, así como también sus principales ventajas y desventajas y sus aplicaciones en la actualidad.

También se trata sobre los protocolos de enrutamiento disponibles para redes WPAN, y de igual forma se hace referencia a los modelos de propagación que se van a utilizar en la elaboración de los escenarios de simulación.

En el cuarto capítulo se presentan los resultados obtenidos de las simulaciones creadas y se realiza el respectivo análisis de la red, tomando para ello ciertos parámetros que previamente son explicados. Finalmente se obtienen las conclusiones y se elaboran las recomendaciones, como resultado del trabajo elaborado.

ÍNDICE DE CONTENIDO

CAPITULO I: INTRODUCCIÓN A WPAN

CAPÍTULO 2: DESCRIPCIÓN DEL ESTÁNDAR IEEE 802.15.4/ZIGBEE

CAPÍTULO 3: CONCEPTOS BÁSICOS SOBRE NETWORK SIMULATOR 2.32

CAPÍTULO 4: ANÁLISIS DEL DESEMPEÑO DE LOS ESCENARIOS DE RED SIMULADOS

CAPÍTULO 5: CONCLUSIONES Y RECOMENDACIONES

ANEXOS

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

GLOSARIO

WPAN: wireless personal area network, redes de area personal inalámbrica
PDA: Personal Digital Assistant, Asistente Digital Personal.
IEEE: Instituto de Ingenieros Eléctricos y Electrónicos
MAC: Medium Access Control, Control de Acceso al Medio
UWB: Ultra Wide-Band
HDVT: high definition televition, televisión de alta definición
BAN: Body Area Network
CSMA-CA: Carrier sense multiple access with collision avoidance, múltiple acceso por detección de portadora evitnado colisiones
RFD: Reduced Funtion Device, dispositivo con funciones reducidas
FFD: Full Funtion Device, dispositivo con funciones completas
SAP: Service Access Point, punto de acceso de servicio
DSSS: direct sequence spread spectrum
BPSK: binary phase-shift keying
O-QPSK: Offset quadrature phase-shift keying
PSSS: Parallel sequence spread spectrum
ASK: amplitude shift keying
ED: energy detection, detección de energía
CCA: Clear Channel Assessment, evaluación de canal despejado
LQI: Link Quality Indication, indicador de calidad de enlace
LLC: Logical Link Control, subcapa de control de enlace lógico
AES: Advance Encryption Standar, estándar avanzado de encriptación
GTS: Guaranteed Time Slots, espacio de tiempo garantizado
APS: Aplication Support Sub-Layer, subcapa de soporte de aplicación
AIB: APS information Base, base de información APS
ZDO: ZigBee Device Object, objeto de Dispositivo ZigBee.
PDU: Protocol Data Units, unidad de datos de protocolos
FCS: Frame Check Sequence, trama de chequeo de secuencia
CRC: Cyclic Redundancy Check, chequeo de redundancia cíclica
SFD: Star of Frame Delimiter, delimitador de Inicio de Trama
CAP: Contention Access Period, Período de Contención de Acceso
CFP: Contention Free Period, Período Libre de Contención
GTS: Guaranteed Time Slot, Espacio Garantizado de Tiempo
VINT: Virtual InterNetwork Testbed
NAM: Network Animador, animador de red
PERL: Practical Extraction and Report Language
DSDV: Destination-Sequenced Distance-Vector Routing Protocol
CGSR: Clusterhead Gateway Switch Routing
WRP: Wireless Routing Protocol
OLSR: Optimized Link State Routing
TBRPF: Topology Dissemination Based on Reverse-Path Forwarding
AODV: Ad Hoc On-Demand Distance Vector Routing
DSR: Dynamic Source Routing
LQSR: Link Quality Source Routing protocol
LMR: Lightweight Mobile Routing
TORA: Temporary Ordered Routing Algorithm
DREAM: Distance Routing Effect Algorithm for Mobility
RREQ: Route Request

RREP: Route Reply
RERR: Route Error

CAPÍTULO 1

INTRODUCCIÓN A WPAN

1.1. DEFINICIÓN DE WPAN

Las redes inalámbricas de área personal (*wireless personal area network*), son redes diseñadas para interconectar y comunicar dispositivos electrónicos tales como PC´s, teléfonos celulares, PDA´s (agendas personales digitales), sensores inalámbricos, impresoras, cámaras fotográficas entre otros dispositivos portables; dentro de un rango de pocos metros **[1].**

En este tipo de redes cada dispositivo puede tener o no movilidad, permitiendo que los usuarios no estén asociados a un punto físico específico dentro de la red. En base a este criterio de movilidad, cuando dos dispositivos con capacidad para WPAN se encuentren lo suficientemente próximos pueden establecer una conexión de manera inmediata, así como también pueden bloquear la comunicación selectivamente con otros dispositivos **[2]**.

Las principales ventajas de este tipo de redes es que no requieren un gran consumo de energía y al momento de su implementación no representan una gran inversión económica, comparada con otras tecnologías; tanto para infraestructura de red como para dispositivos. Sin embargo, las W*ireless PAN* son redes pequeñas con cobertura limitada.

1.2. GRUPOS DE TRABAJO Y ESTÁNDARES IEEE QUE CONFORMAN LAS WPAN

Dentro del Instituto de Ingenieros Eléctricos y Electrónicos (IEEE), existe el grupo de trabajo IEEE 802.15, que esta especializado en redes inalámbricas de área personal (WPAN) **[3]**; a su vez, este grupo se divide en 5 subgrupos de trabajo para proponer y publicar estándares.

1.2.1. *Task Group 1* – IEEE 802.15.1 (WPAN / Bluetooth)

Está basado en los desarrollos de *Bluetooth™ Special Interest Group* (SIG*)*; por lo que el estándar IEEE 802.15.1-2002; publicado el 14 de junio de 2002; es completamente compatible con la especificación Bluetooth v1.1 **[4]**. Incluye recomendaciones para las capas *Medium Access Control* (MAC) y Física, permitiendo un nivel de interoperabilidad que facilite la comunicación de datos entre una WPAN y un dispositivo IEEE 802.11™.

El 14 de febrero de 2005 se publicó, a manera de actualización, el estándar IEEE 802.15.1-2005, que define mecanismos para lograr una mejor transferencia de datos de una WPAN y un dispositivo IEEE 802.11b™ **[5]**.

1.2.2. *Task Group 2* – IEEE 802.15.2 (COEXISTENCIA)

Se encarga de desarrollar prácticas y mecanismos que faciliten la coexistencia de dispositivos para redes WPAN (IEEE 802.15.1) y WLAN (IEEE 802.11b), ya que ambos tipos de redes inalámbricas funcionan en bandas de frecuencias no licenciadas como la de 2.4 GHz. El estándar publicado es IEEE 802.15.2-2003.

La coexistencia se ve afectada principalmente por interferencias mutuas que se producen entre las redes inalámbricas, básicamente por circunstancias como la distancia entre ellas, la cantidad de tráfico de datos que fluyen en las redes y los niveles de potencia de los dispositivos **[6]**.

1.2.3. *Task Group 3* – IEEE 802.15.3 (WPAN de Alta Velocidad)

Surge para crear una WPAN que pueda transmitir datos de una manera más rápida y eficiente. Trabaja en la frecuencia no licenciada de los 2.4 GHz y sin embargo, genera poca interferencia con otras redes como las 802.11b, debido a que sus niveles de transmisión se realizan a niveles menores de potencia.

El estándar IEEE 802.15.3-2003, se encarga de definir las capas Física y MAC para redes WPAN, logrando que puedan alcanzar velocidades de 11, 22, 33, 44 y 55 Mbps y con un rango aproximado de 30 a 50 metros.

- IEEE 802.15.3a (Nivel Físico para WPAN de alta velocidad)

Pretendía ofrecer una alternativa para el nivel físico de UWB[1] (U*ltra Wide-Band*), pero el 19 de enero del 2006 los miembros del grupo se vieron en la necesidad de detener el desarrollo del estándar, debido que a nivel mundial esta nueva tecnología todavía era desconocida, por lo que se optó por esperar unos años para determinar si se continuaría con la elaboración del estándar. **[7]**.

[1] Ultra Wide Band: espectro de RF de gran ancho de banda que permite transmisión de grandes paquetes de datos a cortas distancias y con bajos niveles de potencia. Utiliza el espectro de frecuencia licenciada que va de 3.1 GHz a 10.6 GHz

- IEEE 802.15.3b (Revisión MAC)

IEEE 802.15.3b-2005 busca lograr una mejora para la implementación y la interoperabilidad de la capa MAC. Prácticamente se considera a esta publicación como una enmienda al estándar IEEE 802.15.1-2005, con el cual se trata de corregir errores, aclarar ambigüedades y añadir aclaraciones editoriales **[8]**.

IEEE 802.15.3c (Alternativa de nivel físico basado en ondas milimétricas)

Este grupo de trabajo, el cual se formo en marzo del 2005, brinda una alternativa a nivel de capa física para el estándar 802.15.3-2003, basado en ondas milimétricas.

A partir de la finalización de este estándar, aproximadamente en el mes de mayo de 2008, las WPAN podrán operar en el rango de frecuencia de 57 GHz a 64 GHz, permitiendo una alta coexistencia con otras redes inalámbricas, ya que esta banda no esta en uso actualmente.

Las WPAN de onda milimétrica se caracterizarán por soportar velocidades de transmisión de 1 Gbps para aplicaciones como Internet, *video on demand* (interactividad en televisión digital) y hasta 2 Gbps para aplicaciones como video HDVT (*high definition televition*) en tiempo real y bus inalámbrico de datos para remplazar cables **[9]**.

1.2.4. *Task Group 4 – IEEE 802.15.4 (Low Rate WPAN)*

El estándar 802.15.4-2003 elaborado para WPAN de baja velocidad, presenta lineamientos para implementar redes de bajo costo y bajo consumo de energía. Sin embargo, a partir de marzo de 2004 este estándar se encuentra

suspendido ya que se creo el grupo de trabajo 4b, que es el encargado de actualizarlo y mejorarlo.

- IEEE 802.15.4a (Alternativa de baja velocidad para capa Física)

Sus esfuerzos se centran en permitir comunicaciones con alta capacidad de localización, alto desempeño, ultra baja potencia y escalabilidad a diferentes velocidades de datos.

En el mes de marzo del año 2007, el grupo de trabajo aprobó una enmienda para el estándar IEEE 802.15.4b-2006, pero desafortunadamente, hasta la fecha actual no tiene planificado más reuniones o conferencias para esta actividad **[10]**.

- IEEE 802.15.4b (Mejoras y Aclaraciones)

Surge con la finalidad de realizar mejoras el estándar ya publicado 802.15.4-2003, enfocándose en lo que referente a la reducción de la complejidad innecesaria, aumento de la flexibilidad en el uso de claves de seguridad y en las consideraciones de frecuencias disponibles para nuevas asignaciones.

En el mes de junio del 2006 se aprobó el estándar IEEE 802.15.4b-2006, el cual fue publicado en septiembre del mismo año **[11]**.

1.2.5. *Task Group 5* – IEEE 802.15.5 (WPAN configurada en Malla)

Dentro de este grupo de trabajo se determinan los mecanismos necesarios para habilitar una configuración en malla de una WPAN, a nivel de las capas físicas y MAC. Sin embargo, todavía no se tiene nada aprobado. **[12].**

1.2.6. *Task Group 6* – IEEE 802.15.6 BAN (*Body Area Network*)

Recientemente conformado, permitirá en el futuro definir un estándar para comunicaciones inalámbricas de corta distancia y de gran cercanía o dentro del cuerpo humano. **[13]**.

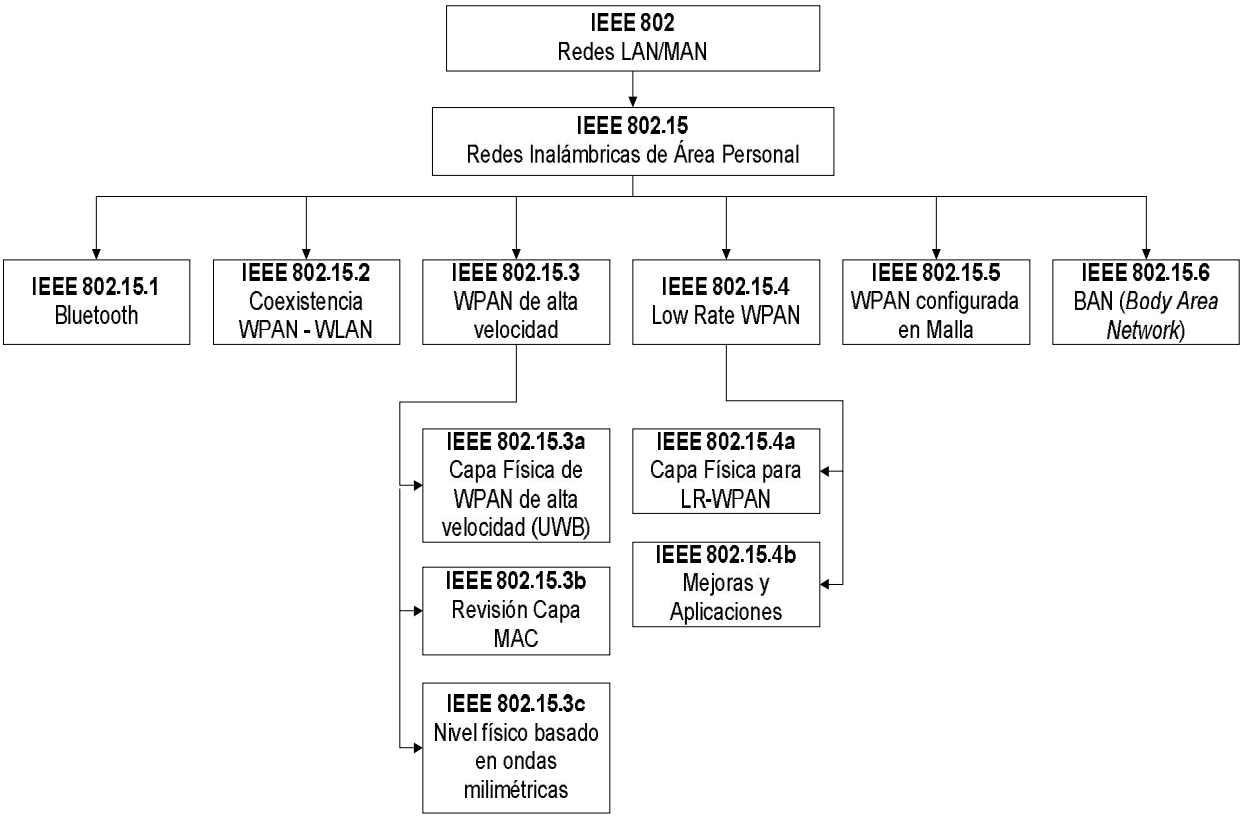


Figura. 1.1. Grupos de Trabajo de IEEE

1.3. TIPOS DE WPAN

Para clasificar las redes WPAN se consideran los siguientes parámetros como la velocidad de transmisión de datos, consumo de energía y la calidad de servicio (QoS). En base a esas características se las clasifican de la siguiente manera:

1.3.1. *High Rate* WPAN

Esta basado en los estándares que han sido publicados por el Grupo de Trabajo 802.15.3 de la IEEE. Gracias a las altas velocidades de transmisión que este tipo de redes permiten manejar, se pueden usara para aplicaciones multimedia que requieren de una calidad de servicio relativamente alta.

1.3.2. *Medium Rate* WPAN

Dentro de este tipo de WPAN se encuentran las redes inalámbricas descritas por el Grupo de Trabajo IEEE 802.15.1 y las especificaciones dadas por *Special Interest Group Bluetooth.* La calidad de servicio que ofrece es óptima y se las aplica principalmente para transmisión de voz, pero también es muy utilizado para transmisiones de datos.

1.3.3. *Low Rate* WPAN

Está dado por el grupo de trabajo IEEE 802.15.4 junto con la colaboración de *ZigBee Alliance,* conjuntamente permiten crear redes con equipos de bajo consumo de energía y una calidad de servicio adecuada principalmente para tráfico de datos por periodos o en intervalos de tiempo **[14][15]**.

1.4. APLICACIONES

Actualmente el uso de redes de área personal ha crecido y se ha dado a conocer gracias a la gran variedad de posibles aplicaciones en las que se las puede utilizar. Es así que, dependiendo del tipo de WPAN, se puede referir algunas aplicaciones como las siguientes:

§ Bluetooth: gracias a su bajo consumo de energía y su aceptable ancho de banda posee una gran cantidad de aplicaciones, entre las que están:

- Conexión de celulares para transferir música e imágenes, además de permitir la conexión con manos libres o audífonos.
- Conexión entre PC´s o laptops con dispositivos periféricos como impresoras, mouse, teclado, cámaras digitales, etc
- Reemplazo para algunas comunicaciones tradicionales como GPS o instrumentos médicos
- Utilización de dispositivos como control remoto, sobre todo para controlar la PC
- Establecimiento de conexiones tipo Chat entre dispositivos bluetooth, permitiendo incluso una comunicación de voz e imágenes en tiempo real
- Dentro del área de entretenimiento, las nuevas consolas de video juegos tienden a usar palancas con tecnología bluetooth para eliminar cables y permitir que más jugadores se enlacen al mismo tiempo **[16].**

§ ZigBee: recientemente utilizado para aplicaciones que implican sensores inalámbricos, debido a que consume menos energía que los dispositivos bluetooth, algunas de sus aplicaciones son:

- Domótica, para control total de viviendas.
- Creación de edificios inteligentes, realizando automatización de luces y control de accesos a los diferentes pisos.

- Se usa para ciertos instrumentos médicos de monitoreo.

- Dentro de redes de sensores inalámbricos para controles de temperatura, presión, tráfico, etc. **[17]**

CAPÍTULO 2

DESCRIPCIÓN DEL ESTÁNDAR IEEE 802.15.4/ZIGBEE

2.1. INTRODUCCIÓN

La tendencia global en la actualidad se ve enfocada a la creación de redes inalámbricas de área personal de bajo costo y con consumo mínimo de energía, siendo la tecnología Bluetooth la más representativa dentro de las WPAN.

A finales del año 2004 se aprobaron las primeras especificaciones creadas por el grupo de desarrollo *ZigBee Alliance*, que se encuentra conformado por más de 100 empresas, con la finalidad de plantear los lineamientos para desarrollar redes de bajo costo, que sean sencillas de implementar y que aprovechen de manera eficiente la vida útil de las baterías que emplean sus nodos.

El desarrollo de la tecnología ZigBee esta basado en el estándar IEEE 802.15.4, el cual sirve de apoyo sobre todo para las capas inferiores de su pila de protocolos, mientras que de las capas superiores se encargan las recomendaciones publicadas por *ZigBee Alliance*, siendo las últimas aprobadas en el año 2006.

ZigBee se encuentra en creciente incremento y difusión; de tal forma, que en la actualidad cuenta con millones de dispositivos en uso alrededor del mundo, permitiendo implementar aplicaciones dentro del área de la domótica, monitoreo con sensores inalámbricos, rastreo en tiempo real, periféricos para computadoras y dentro del entretenimiento para crear cámaras fotográficas, PDAs, celulares y

juguetes, dentro de los video juegos para permitir que varias consolas se puedan enlazar e implementar controles inalámbricos para múltiples jugadores **[19]**.

2.2. CARACTERÍSTICAS PRINCIPALES

Para conocer las características que definen a las *Low Rate WPAN,* se las puede dividir en las que proporciona el estándar IEEE 802.15.4 y las que están dadas por la *ZigBee Alliance*.

2.2.1. Características de IEEE 802.15.4

§ Trabaja a nivel de capa física y subcapa MAC (*Medium Access Control*)

§ Opera en la banda de frecuencia libre ISM, para usos médicos, científicos e industriales, que corresponde a 2.4 GHz a nivel mundial. En Europa se usa la banda de 868 MHz y la banda 915 MHz en USA.

§ Permite implementar redes con topología estrella o punto a punto

§ Maneja el direccionamiento a nivel de capa MAC (dirección MAC reducida de 16 Bits o dirección MAC extendida de 64 Bits)

§ No requiere un alto consumo de energía, empleando 30mA para transmisión y 3uA en reposo.

§ Utiliza *Carrier sense multiple access with collision avoidance (CSMA-CA)*, como método para acceder al medio de transmisión

§ Maneja hasta 65536 nodos, distribuidos dentro de hasta 255 subredes

§ El rango de cobertura o área de influencia es en promedio de 75 metros

§ Soporta velocidades de transmisión de 20kbps, 40kbps y 250kbps.

2.2.2. Características de ZigBee

§ Maneja las capas superiores de la pila de protocolos, como son la capa de red y la de aplicación

§ Se encarga del enrutamiento de paquetes

§ Utiliza direcciones de capa de red de 16 bits

§ Permite la creación de una PAN con topologías en malla gracias a que puede manejar funciones de enrutamiento **[20]**.

2.3. TIPOS DE NODOS

Tanto el grupo de trabajo IEEE 802.15.4 como ZigBee Alliance, definen diferentes tipos de nodos dentro de sus publicaciones, dependiendo de las funciones que desempeñan dentro de la red inalámbrica. Sin embargo, cada dispositivo tiene su correspondiente en el otro estándar y lo único que varía es el nombre que se le otorga.

2.3.1. Nodos Definidos por *ZigBee Alliance*

§ **Coordinador ZigBee (CZ)**

Es el encargado de iniciar la formación de la red inalámbrica, escoge un canal libre y lo administra, selecciona un identificador de red (PAN ID) y posteriormente puede actuar como router. También actúa como centro de validación (*trust center)* que es el que permite que un nodo permanezca en la red y pueda intercambiar datos mediante una clave de red, o caso contrario se lo fuerce a salir.

Por otro lado, el coordinador ZigBee es el encargado de controlar el proceso de incorporación de nuevos dispositivos, tomando en cuenta los parámetros iniciales de configuración de la red y manejando las peticiones de los nuevos dispositivos.

Mantiene una lista de los dispositivos incorporados y brinda soporte a dispositivos libres para que puedan asociarse o reincorporarse a la red.

Como controlador de las incorporaciones de dispositivos, también puede eliminarlos o desasociarlos, previa petición de los mismos.

- **Router ZigBee (RZ)**

Una vez que el router ha sido validado y asociado a la red, será el encargado de permitir que otros dispositivos se incorporen a dicha red, mediante los parámetros de configuración que posee. Sin embargo, este dispositivo es opcional ya que el coordinador de red puede cumplir con la función de enrutar paquetes.

Cuando el router recibe una petición de un nuevo nodo para unirse a la red, es el encargado de comunicarlo al coordinador y si la seguridad de red está habilitada, dicha petición deberá pasar por el centro de validación. Una vez que se permita su asociación el router debe indicarle al nuevo nodo la configurar de la red.

El router mantiene una lista de los nodos asociados, con la finalidad de enrutar paquetes. De igual manera, también puede eliminar o quitar nodos de la porción de red que esta bajo su cargo.

§ **Dispositivo Final – End Device ZigBee (EDZ)**

Son los dispositivos restantes que participan en la red pero que no son ni el coordinador ni los routers, por lo tanto no pueden enrutar paquetes y tampoco asociar nuevos nodos.**[21]**

2.3.2. Nodos Definidos por las Recomendaciones IEEE 802.15.4

Este grupo de trabajo define dos tipos de nodos que participan dentro de una red inalámbrica y que son:

§ **Dispositivos con Funciones Reducidas (*RFD - Reduced Funtion Device*)**

Es un dispositivo para aplicaciones sencillas que no necesitan enviar o recibir grandes cantidades de datos. Su instalación es sencilla y de bajo costo, y gracias a su poca complejidad su consumo energético es reducido.

Sin embargo, solo pueden comunicarse con el dispositivo FFD que actúa como coordinador de red, que será el encargado de gestionar sus peticiones. Esto limita a los RFD a estar únicamente dentro de una topología de red en estrella.

§ **Dispositivos con Funciones Completas (*FFD – Full Funtion Device*)**

Funciona como coordinador, ruteador o terminal, ya que posee memoria extra y capacidad computacional, permitiéndole cumplir con la tarea de enrutar paquetes. Puede comunicarse con otros FFD o con RFD, posibilitando configurar cualquier topología de red.**[22]**

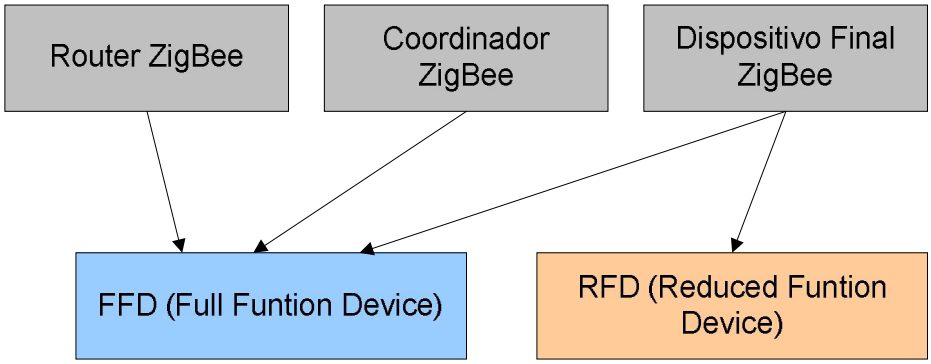


Figura. 2.1. Tipos de Dispositivos IEEE 802.15.4/ZigBee

2.4. TOPOLOGÍAS DE RED

2.4.1. Topología Estrella

Se configura con un único coordinador de red y varios dispositivos de funciones reducidas (RFD), también pueden existir varios dispositivos de funciones completas pero que no actúen como coordinador o router.

El coordinador será el encargado de comunicar a todos los demás dispositivos de la red, esto gracias a que mantiene tablas de relaciones o direccionamiento directo, que le permite determinar cual es el destino de un determinado paquete.

Cada red en estrella trabaja independientemente de cualquier otra que se encuentre en su rango de cobertura, debido a que al iniciarse la configuración de la red, el coordinador escoge un PAN ID que no este siendo usado por otro coordinador próximo.

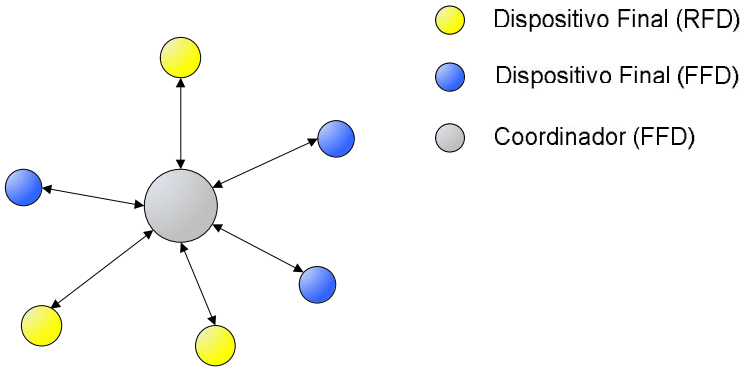


Figura. 2.2. Topología en Estrella

2.4.2. Topología Punto a Punto

Se encuentra conformado igualmente por un solo coordinador de red, pero con la diferencia que cada dispositivo final es un FFD que puede establecer enlaces punto a punto hacia los otros nodos, razón por lo cual pueden comunicarse entre todo ellos.

Al inicio el coordinador será el encargado de formar la red y de enrutar los paquetes, pero conforme se establecen los nodos, estos serán capaces de realizar el encaminamiento de los datos a su destino, incluso mediante múltiples saltos.

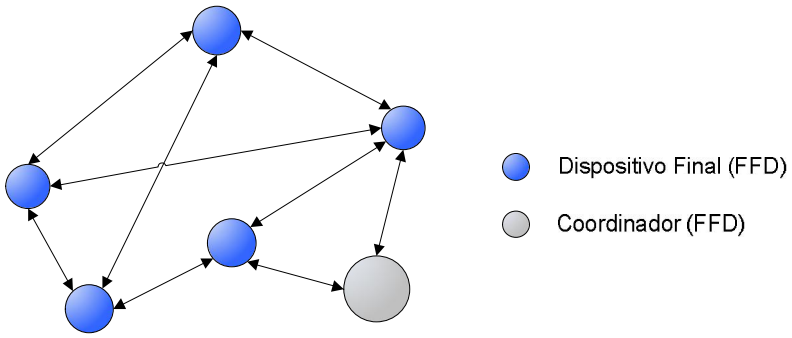


Figura. 2.3. Topología Punto a Punto (Peer-to-Peer)

2.4.3. Topología Malla

Es una extensión de la red punto a punto, con la diferencia que a cada FFD que conforma la red, se le agregan dispositivos finales RFD. De esta manera aparecen los llamados Router ZigBee que permitirán comunicar a los nodos entre si.

Este tipo de topología permite mantener una baja latencia y una alta confiabilidad; sin embargo, se requiere de dispositivos con mayor capacidad computacional para manejar datos y enrutamiento.

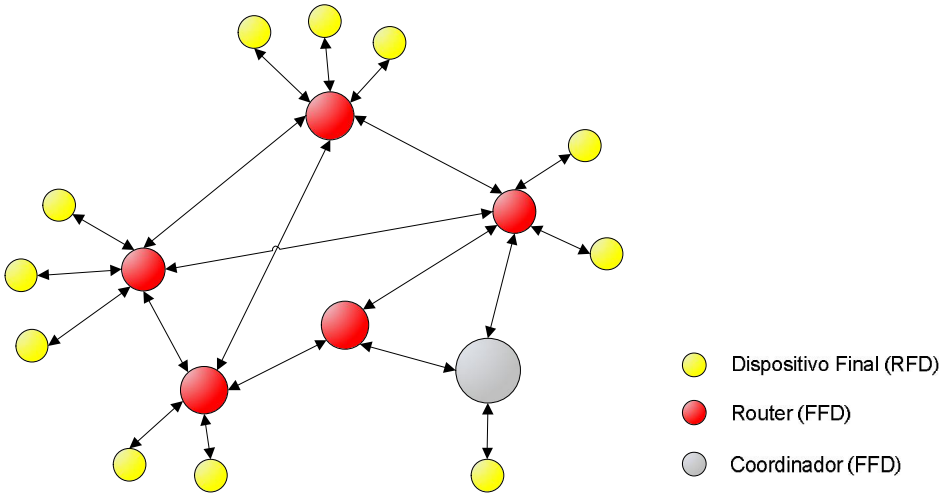


Figura. 2.4. Topología en Malla

2.5. ARQUITECTURA

Como se ha venido mencionando, las capas inferiores de los dispositivos ZigBee, están basadas en las especificaciones IEEE 802.15.4. Mientras que, las capas superiores corresponden a las publicaciones realizadas por *ZigBee Alliance.*

El modelo por capas de IEEE802.15.4/ZigBee esta basado en el Modelo OSI (*Open Systems Interconnection*); de tal forma que la Capa Física (PHY) y la Subcapa de Control de Acceso al Medio (MAC) están determinadas por las especificaciones del grupo de trabajo IEEE 802.15.4.

La Capa de Red (NWK) y la Capa de Aplicación (APL) están dadas por las publicaciones que realiza el grupo de empresas *ZigBee Alliance.* A su vez la Capa de Aplicación consta de una Subcapa de Soporte de Aplicación (APS), Objetos para dispositivos ZigBee (ZDO) y Entorno de Aplicación (AF) dentro del cual están los Objetos de Aplicación que son definidos por el desarrollador.

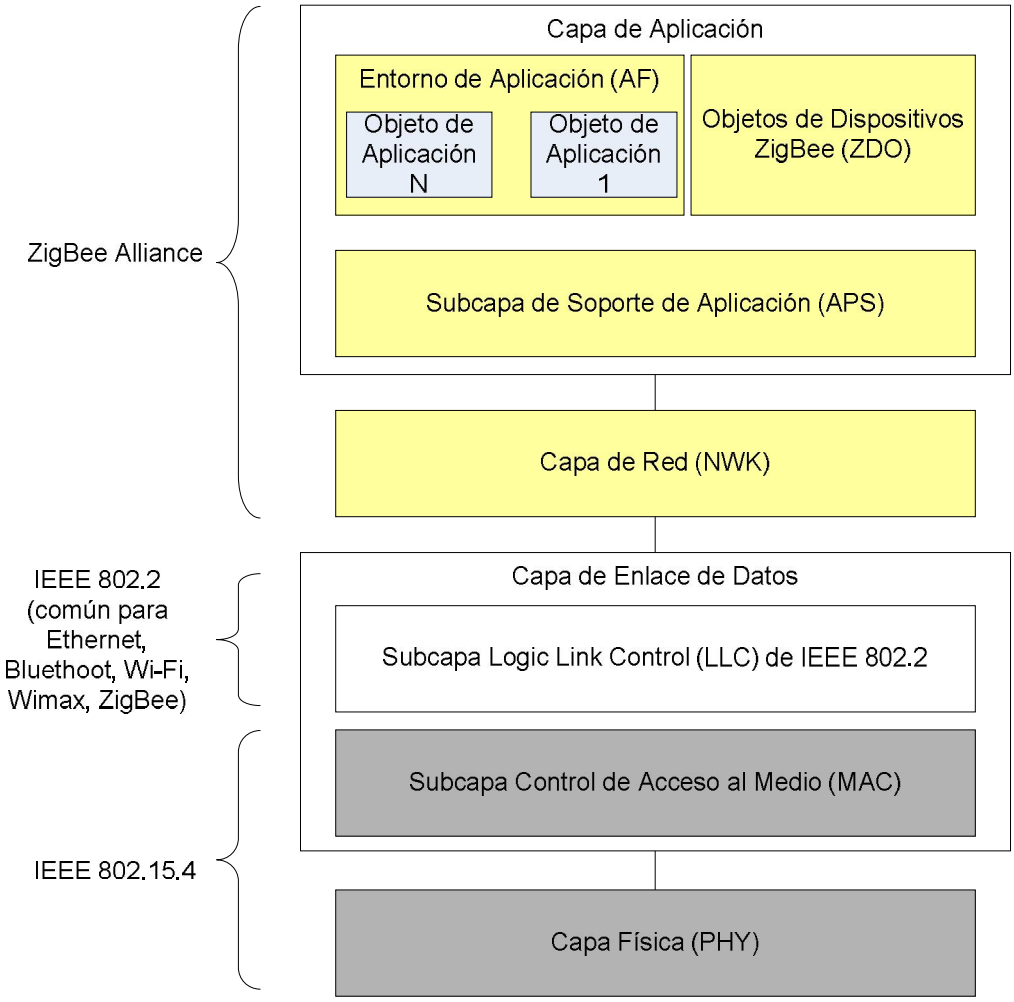


Figura. 2.5. Modelo de Capas o Pila de ZigBee

Cada capa posee un determinado número de servicios, que pueden ser para la transmisión de datos o para administrar el dispositivo. A su vez, cada capa posee una interfase que le permite enlazarse a la capa superior conocido como *Service Access Point* (SAP), y cada SAP posee un número de primitivas de servicios que le permiten cumplir con las funciones requeridas

A continuación se detalla las características y funciones de cada capa que conforma la pila de IEEE 802.15.4/ZigBee:

2.5.1. Capa Física (*Physic Layer, PHY*)

Se encuentra definida en el estándar IEEE 802.15.4-2006, en el cual se hace referencia a la existencia de cuatro tipos de capas físicas y cuya elección dependen del usuario, basado en la ubicación geográfica de la red. Las capas físicas se diferencian principalmente por la frecuencia con la que trabajan, teniendo de esta manera las siguientes:

§ Capa Física que trabaja a 868/915 MHz con Secuencia Directa de Espectro Ensanchado (DSSS – *direct sequence spread spectrum*) y que emplea modulación BPSK (*binary phase-shift keying)*

§ Capa Física que trabaja a 868/915 MHz con DSSS y modulación O-QPSK (*Offset quadrature phase-shift keying*)

§ Capa Física que trabaja a 868/915 MHz con el método *Parallel sequence spread spectrum* (PSSS) y que emplea modulación BPSK y ASK (*amplitude shift keying*)

§ Capa Física que trabaja a 2.4 GHz con DSSS y modulación O-QPSK.

Según la publicación del año 2003, la banda de frecuencia de 868 – 868.6 MHz, que es usada en Europa posee un canal, permitiendo velocidades de transmisión de 20 Kbps. Por otra parte, la banda de 915 - 928 MHz, que es usada en América del Norte posee 10 canales con espaciamiento de 2 MHz, permite una velocidad de transmisión de 40 Kbps. Dentro de la banda de 2.4 – 2.4835 GHz, que es usada en el resto del mundo, cuenta con 16 canales con espaciamiento entre ellos de 5 MHz, permitiendo manejar velocidades de transmisión de 250 Kbps.

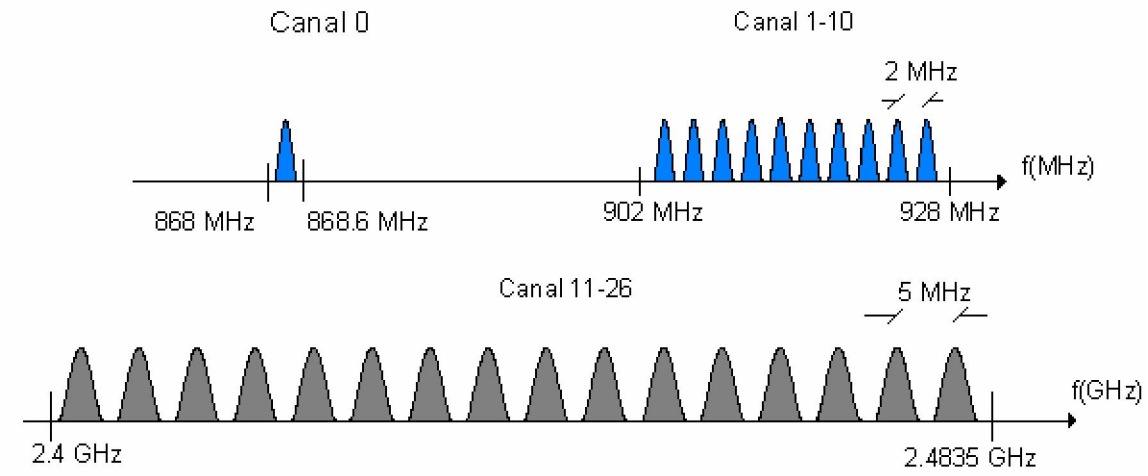


Figura. 2.6. Canales de Frecuencias usadas por IEEE 802.15.4-2003

Tabla. 2.1. Capa Física IEEE 802.15.4-2003

Capa Física	Lugar en la que se usa	Velocidad de bits	Canales	Espaciamiento entre canales
868 - 868,6 MHz	Europa	20 Kbps	1	-
902 - 928 MHz	América del Norte	40 Kbps	10	2 MHz
2,4 - 2,4835	Resto del Mundo	250 Kbps	16	5 MHz

Con la agregación de dos tipos más de capas físicas opcionales en la publicación del estándar IEEE 802.15.4-2006; es necesario un mejor uso de los 32 bits para la asignación de canales. La forma que se encontró para solucionar la necesidad de incrementar el número de canales por banda de frecuencia fue la de considerar a los 5 bits mas significativos como un número de página (*channel page*), mientras que los restantes 27 bits representarían el número de canal (*channel number*).

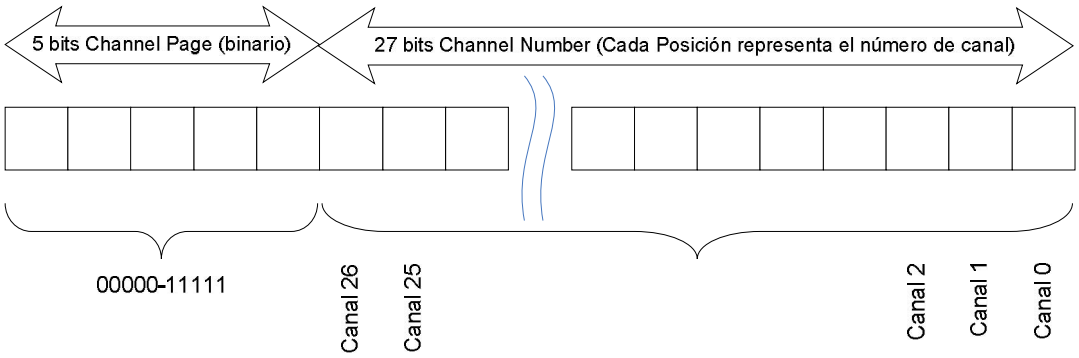


Figura. 2.7. Campo de 32 bits para asignación de Canales y Páginas según IEEE 802.15.4-2006

De esta forma se tiene en total 31 páginas, cada una con 27 canales; sin embargo solo se pueden usar las tres primeras páginas ya que las restantes están reservadas para futuras aplicaciones.

Tabla. 2.2. Channel Page y Channel Numbers

Channel Page (Decimal)	Channel Page (Bianrio) (b31,b30,b29,b28,b27)	Channel Number (Decimal)	Descripción
0	0 0 0 0 0	0	Canal 0 en la banda 868 Mhz que usa BPSK
		1 - 10	Canal 1 al 10 en la banda 915 Mhz que usa BPSK
		11 - 26	Canal 11 al 26 en la banda 2,4 Ghz que usa O-QPSK
1	0 0 0 0 1	0	Canal 0 en la banda 868 Mhz que usa BPSK
		1 - 10	Canal 1 al 10 en la banda 915 Mhz que usa BPSK
		11 - 26	Reservado
2	0 0 0 1 0	0	Canal 0 en la banda 868 Mhz que usa BPSK
		1 - 10	Canal 1 al 10 en la banda 915 Mhz que usa BPSK
		11 - 26	Reservado
3 - 31	0 0 0 1 1 - 1 1 1 1 1	Reservado	Reservado

Tabla. 2.3. Capa Física IEEE 802.15.4-2006

Capa Física (MHz)	Banda de Frecuencia	Lugar en la que se usa	Velocidad de bits	Modulación
868/915	868 - 868,6 MHz	Europa	20 Kbps	BPSK
	902 - 928 MHz	América del Norte	40 Kbps	BPSK
868/915 (opcional)	868 - 868,6 MHz	Europa	250 Kbps	ASK
	902 - 928 MHz	América del Norte	250 Kbps	ASK
868/915 (opcional)	868 - 868,6 MHz	Europa	100 Kbps	O-QPSK
	902 - 928 MHz	América del Norte	250 Kbps	O-QPSK
2450	2,4 - 2,4835 GHz	Resto del Mundo	250 Kbps	O-QPSK

La capa física también es responsable de manejar tareas específicas como las siguientes:

§ Se encarga de activar y desactivar el *transceiver* de ondas de radio, para la transmisión y recepción.

§ Detecta el nivel de energía (*energy detection* - ED) en el canal que se encuentra en uso, esto para determinar sí está llegando información al nodo, o sí este puede pasar a estado pasivo después de un tiempo de no recibir señal.

§ Evaluar sí el canal esta despejado (CCA – *Clear Channel Assessment*) proporcionando información validad que será usado por el algoritmo CSMA – CA (*carrier sense multiple access with collision avoidance*)

§ Indica la calidad del Enlace (*Link Quality Indication,* LQI), basado en el nivel de energía de recpción o en estimaciones de la relación de señal a ruido, este indicador es usado en capas superiores como la de Red o de Aplicación

§ Selecciona la frecuencia del canal a ser usado

§ Realiza la recepción y transmisión de bits **[23]**

2.5.2. Capa de Enlace de Datos (*Data Link Layer, DDL)*

Esta capa se encuentra dividida en dos subcapas, siendo una de ellas la de Control de Enlace Lógico (*Logical Link Control, LLC*), que se encuentra definida dentro de las publicaciones del grupo IEEE 802.2, y que es común para otros tipos de tecnologías de acceso como Ethernet, Bluetooth, Wi-Fi, WiMax y ZigBee.

La otra subcapa es la de Control de Acceso al Medio (*Medium Access Control, MAC*) que depende del tipo de hardware que se encuentre en la capa física. En este caso la subcapa se encuentra definida dentro del estándar IEEE 802.15.4-2006, y que sirve de enlace entre la capa física y la subcapa LLC.

Dentro de las funciones que cumple la subcapa MAC están las siguientes:

- Manejar todos los tipos de accesos al canal físico de radio

- Soportar las agregaciones y desagregaciones de nodos dentro de la PAN. También implementa procesos para permitir la reasociación de nodos que anteriormente ya pertenecían a la PAN

- Brinda tres tipos de seguridad a nivel de subcapa MAC que son: sin seguridad (para aplicaciones de anuncios publicitarios), mediante la aplicación de listas de control de acceso (sin encriptación) y un modo seguro con uso de claves, mediante el estándar de encriptación simétrico AES 128 (*Advance Encryption Standar)*, es decir que las dos partes negociarán una subclave cifrada de 128 bits a partir de una clave original, para permitir el envió y la recepción de mensajes.

- Es responsable de la identificación de los nodos en base a direcciones extendidas de 64 bits, que pueden ser usadas en el proceso de asociación; o direcciones cortas de 16 bits, que son usadas por el coordinador de red para la comunicación con otros dispositivos de la red

- Permite realizar la sincronización de la red, ya sea mediante beacons, o en caso de no utilizarlos se realiza directamente intercambiando datos entre el coordinador y el nodo

- Para redes que no utilizan beacons, emplea como mecanismo de acceso al canal el algoritmo CSMA-CA "*Carrier Sense Multiple Access with Collision Avoidance" (*acceso múltiple por detección de portadora con evasión de colisiones)

- Dentro de redes que empelan beacons, utiliza el mecanismo de espacios de tiempo garantizados *(Guaranteed Time Slots, GTS*); es decir que a cada nodo se le asignará un determinado espacio de tiempo dentro de una Supertrama, en el cual podrá transmitir sin latencia y aprovechando al máximo el ancho de banda. **[24]**

2.5.3. Capa de Red (*Network Layer, NWK)*

La capa de Red se encuentra especificada dentro de las publicaciones de la ZigBee Allinace, que en general busca cumplir con los mismos objetivos de otras capas de red en otros modelos; es decir, entregar los datos generados en las capas superiores al dispositivo destinatario dentro de la red, con la diferencia que también se encarga de no generar un consumo de energía elevado, esto gracias a que puede activar o desactivar su hardware de recepción, permaneciendo la mayor parte del tiempo dormido y reaccionando únicamente ante peticiones de transmisión o recepción

Dentro de las funciones y responsabilidades de la Capa de Red se encuentran las siguientes tareas, tanto para la transmisión de datos como para administrar el dispositivo:

- En lo referente a la transmisión de datos es el encargado de enviar los paquetes al destino final, o de ser el caso al dispositivo del salto siguiente (*next hop*), que permitirá alcanzar el destino final. Esto gracias a que maneja

protocolos de enrutamiento que le permiten mantener una topología de red o conocerla a través de la información que le envían los vecinos.

- Brinda seguridad gracias a la capacidad de permitir autentificación y confidencialidad de la transmisión

- Dentro de los servicios de administración del dispositivo, la capa de red permite la configuración de su pila en base a los requerimientos de operación. Es decir, administra opciones de configuración que le permitirán al dispositivo iniciar sus actividades como Coordinador ZigBee o simplemente unirse a una red existente.

- Si el dispositivo es un Coordinador o un Router ZigBee, esta capa le permitirá administrar la asociación, reasociación o la salida de un nodo en base a las peticiones que recibe del otro dispositivo.

- Para el caso de Coordinadores o Routers ZigBee, se encarga de la asignación de direcciones a los dispositivos que se asocian a la red

- Es la capa encargada de descubrir, almacenar y reportar información a los dispositivos vecinos que se encuentran directamente a un salto (*next hop*)

- Maneja el control de recepción, que es la capacidad que tiene un dispositivo de activar su receptor en un tiempo determinado, para permitir que se produzca la sincronización a nivel de subcapa MAC o directamente la recepción de datos

- Soporta varios mecanismos de enrutamiento como *broadcast, multicast* y *unicast*; para permitir un intercambio de información dentro de la red

2.5.4. Capa de Aplicación (*Aplication Layer,* APL)

La capa de aplicación se encuentra dividida en tres subcapas de la siguiente manera y que se puede apreciar en la figura 2.8:

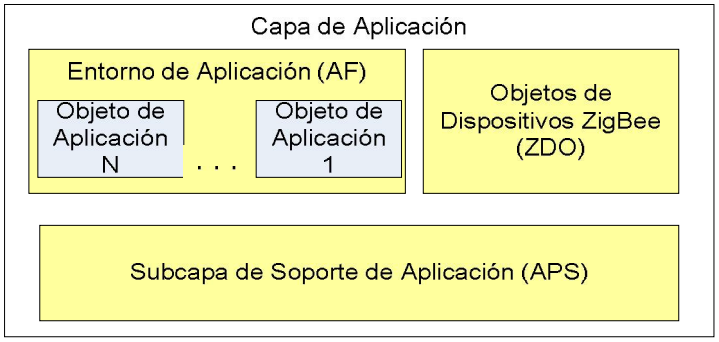


Figura. 2.8. Capa de Aplicación

- Subcapa de Soporte de Aplicación (*Aplication Support Sub-Layer*)

Es la encargada de brindar una interfase que permita enlazar la Capa de Red y la Capa de Aplicación. Al igual que las otras capas, consta con servicios tanto para datos como para control o administración, siendo los siguientes los más importantes:

- Se encarga de la vinculación entre dos dispositivos, generando mensajes que serán transmitidos de un dispositivo al otro. La manera de vincular a dos dispositivos en base a los servicios y necesidades requeridas

- Aumenta la confiabilidad del enlace establecido por la capa de Red, mediante el mecanismo de reenvío punto a punto (*end-to-end retries*)

- Controla que los mensajes de transmisión o retransmisión no sean recibidos mas de una vez

- Permite la fragmentación y el ensamblaje de datos, en el caso en que se exceda la cantidad de bits permitidos en la Capa de Red

- Mantiene y controla una base de datos de los objetos administrados llamada APS *information Base* (AIB)

- La seguridad en esta capa es mediante la implementación de una autenticación con los otros dispositivos a través de *secure keys*

- Tiene la capacidad de asignar una única dirección compartida por varios dispositivos, con la finalidad de administrarlos a manera de grupo

- Entorno de Aplicación (*Aplication Framework,* AF)

Es el medio en el cual se encuentran hospedados los objetos de aplicación, que representan el software que ha sido desarrollado por el fabricante para que el dispositivo cumpla con funciones y tareas específicas.

Dentro de cada dispositivo existe la posibilidad de configurar hasta 240 objetos de aplicación, desarrollados por el fabricante o adquiridos a otros desarrolladores. Cada objeto tiene un número que lo identifica del 1 al 240 y se a reservado el número 0 para una interfase de datos hacia la ZDO (*ZigBee Device Object)* y el número 255 para una interfase de datos con funciones de broadcast hacia todos los objetos de aplicación.

- Objeto de Dispositivo ZigBee (*ZigBee Device Object,* ZDO*)*

Representa la parte de la pila de ZigBee que se encarga de todo lo referente a la administración y control del dispositivo, además de manejar lo relacionado a las políticas de seguridad que serán ejecutadas por las capas inferiores. De esta manera cumple con las siguientes funciones:

- Se encarga de inicializar la Subcapa de Soporte de aplicación (APS), así como también la capa de Red (NWK) y todos los servicios de seguridad.

- Maneja la información para determinar e implementar el proceso de descubrimiento, asociación, seguridad y administración de red

- Dentro de la administración de la seguridad permite que se habiliten o se deshabiliten conjuntamente con las otras capas, controlando el establecimiento, transporte, actualización, cambio y remoción de claves, así como también la autenticación de los dispositivos

- Para la administración de red se encarga de permitir la selección del canal para iniciar la formación de la PAN (para coordinador ZigBee) o detecta la PAN a la que quiere unirse, también detecta interferencias en el canal para un posible cambio de frecuencia. De igual forma, detecta redes vecinas e identifica a su respectivo router o coordinador de red

2.6. ESTRUCTURA DE LAS PDU DE ZIGBEE

Cada capa en la arquitectura ZigBee/802.15.4 a más de cumplir con sus funciones específicas, también se encarga de generar su propio PDU (*Protocol Data Units)* el cual posee varios campos de datos que serán enviados a la capa inferior siguiente, para que esta a su vez le adjunte su propio PDU y de igual forma le pase a su capa inferior.

En el proceso de transmisión los datos se forman en las capas superiores y van descendiendo por las restantes capas. Mientras que en la recepción, la información llega a las capas inferiores primero y va subiendo hasta llegar a la aplicación que se encargará de ejecutar la tarea específica.

2.6.1. PDU de la Capa de Aplicación

La subcapa de Soporte de Aplicación es la encargada de generar el respectivo PDU por lo que toma el nombre de ASPDU. Los siguientes campos son los que conforman el ASPDU:

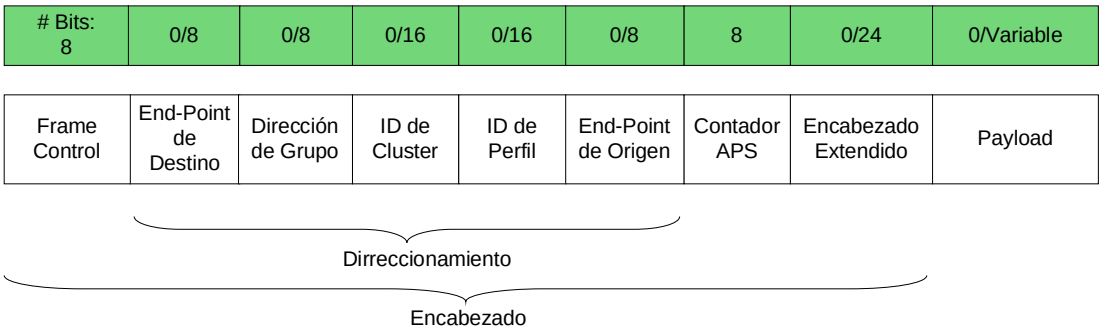


Figura. 2.9. PDU de la Capa de Aplicación ZigBee (ASPDU)

Frame Control: tiene una longitud de 8 bits, que se encuentran agrupados en subcampos o banderas (*Flags)* los cuales indican el tipo de la trama, tipo de entrega, seguridad entre otros.

Figura. 2.10. Banderas del Campo "Frame Control"

- *Tipo de Trama:* Consta de 2 bits y especifica el tipo de trama que se recibe o envía, basado en la siguiente tabla:

Tabla. 2.4. Bits del Tipo de Trama

Bits del Tipo Frame b1 b0	Tipo de Frame
0 0	Dato
0 1	Comandos
1 0	ACK
1 1	Reservado

- *Modo de Entrega:* Consta de 2 bits y especifica como será la entrega de las trama, se basa en la siguiente tabla:

Tabla. 2.5. Bits para el Tipo de Entrega de la Trama

Bits de Tipo de Entrega b1 b0	Tipo de Entrega
0 0	Entrega normal unicast
0 1	Indirecto
1 0	Broadcast
1 1	Direccionamiento en Grupo

- *Formato ACK:* Este bit determina si se enviarán los campos de End-Point de destino, ID de Cluster, ID de perfil y End-Point de Origen en una trama Acknowledgement o de acuse de recibo. El bit debe ser puesto en cero (0) para que se de esta situación

- *Seguridad:* Es un bit que permitirá administrar el perfil de seguridad de la capa de aplicación

- *Solicitud ACK:* este bit determina la necesidad de enviar una respuesta ACK (acuse de recibo) al dispositivo que origino la trama. En el caso que se encuentre en 1, se necesita armar una trama ACK después de que se ha

recibido los datos y se los considera válidos. En el caso que el valor sea 0, no se originará ningún ACK de respuesta.

- *Presentación de Encabezado Extendido:* Si el bit se encuentra en 1, se indica que la trama contendrá un encabezado extendido

End-Point de Destino: Cada dispositivo tiene la posibilidad de manejar hasta 240 *End-Points* que son aplicaciones separadas que comparte el mismo canal de radio y *transceiver* para su transmisión. Al poseer cada dispositivo una única dirección física, las direcciones de *End-Point* son las que permiten que cada aplicación se comunique directamente con otras aplicaciones con la misma dirección de *End-Point.*

Específicamente este campo de 8 bits de longitud permite seleccionar el *End-Point* en el dispositivo de recepción, al que será enviada la trama. Por lo que este campo estará presente únicamente cuando el sub-campo de tipo de entrega de trama sea unicast, indirecta (ya que uno de los parámetros requeridos es la dirección de *End-Point*) y para el caso de broadcast. Parar la entrega unicast e indirecta el campo puede tomar un valor comprendido entre 0x01 (1) a 0xf0 (240), todos los *End-Point* con números 0xf1-0xfe son reservados. Mientras que, para broadcast la dirección a usarse el la 0xff.

Dirección de Grupo: Tiene una longitud de 16 bits, que representa a una dirección de grupo para todos los *End-Points* que comporten un mismo ID de grupo. Este campo pude estar presente solamente si el sub-campo de tipo de entrega esta seleccionado para direccionamiento en grupo. En este caso el campo de “End-Point de destino” no constará en la trama.

Identificador de Cluster: El *cluster* es el conjunto de uno o más atributos, que son datos de una aplicación. Cada *cluster* posee un identificador único dentro del perfil al que pertenece, mediante el cual se puede comunicar con su respectivo *cluster* en el *end-point* de recepción. El campo de ID de Cluster consta de 16 bits y solo se le encuentra en tramas de datos y ACK.

Identificador de Perfil: Cada dispositivo puede soportar varios perfiles, por lo que este campo de 16 bits permite identificar hacia o desde que perfil ha sido creada la trama. Únicamente se encuentra presente en tramas de datos y ACK.

Un perfil es la base para que se pueda dar la comunicación entre dos dispositivos sin importar el fabricante, trabajan juntos para cumplir con una aplicación distribuida en la red. Cada perfil es un mecanismo para que distintos dispositivos sean compatibles, pudiendo definir por ejemplo el método de comunicación, el tipo de mensaje que se usará, los comandos disponibles, las respuestas que se deben obtener, etc.

Existen perfiles públicos que son desarrollados por alguna empresa perteneciente a la ZigBee Alliance y que ha pagado para que este perfil pueda ser aprobado y usado por otras empresas permitiendo crear dispositivos compatibles. También existen perfiles que son propietarios y que únicamente funcionan para dispositivos de una misma marcar y que son creados cuando los perfiles públicos no cumplen con sus expectativas.

End-Point de Origen: tiene una longitud de 8 bits, e indica la dirección del End-Point que ha originado la trama.

Contador APS: posee una longitud de 8 bit y sirve para prevenir la recepción de tramas duplicadas. El valor en este contador es incrementado con cada nueva transmisión

Encabezado Extendido: Consta de tres octetos que permiten determinar sí la información esta fragmentada, así como también el número de fragmentos totales, el número del fragmento actual y sí cada fragmento a llegado con éxito al receptor.

Payload: Este campo es de longitud variable, y depende del tipo de trama que se este enviando, los cuales pueden ser de datos, comandos o tramas ACK (no contiene payload, únicamente el respectivo encabezado).

2.6.2. PDU de la Capa de Red

La PDU de la capa de red se la conoce como NPDU, y se encarga de agregarle ciertos campos de encabezado, a la información que le llega de la capa de aplicación. La NPDU se estructura de la siguiente manera:

Figura. 2.11. PDU de la Capa de Red (NPDU)

Frame Control: Tiene una longitud de 16 bits, que permiten definir el tipo de trama (datos o comandos de capa de red), la versión del protocolo que utiliza la capa de red, un subcampo para saber si la trama será enviada en unicast, broadcast o multicast, también permite conocer si se encuentra habilitada o no la seguridad a nivel de esta capa. Determina si se utilizará direcciones IEEE o no, tanto para direcciones de origen como de destino.

Dirección de Destino: Es un campo de 16 bits de longitud que siempre está presente. Si dentro del campo Frame Control, la bandera que indica que el envío será unicast o broadcast esta desactivada, la dirección de destino será la correspondiente al dispositivo de destino o a la dirección de broadcast; pero si la bandera esta activada, esta campo de dirección destino mantendrá los 16 bits del ID de Grupo que le envía la capa superior

Dirección de Origen: De igual forma que el campo anterior, tiene una longitud de 16 bits y siempre está presente. Corresponde a la dirección del dispositivo que envía la trama o el ID de Grupo.

Radio: Es un campo de 8 bits de longitud que está siempre presente y que indica la cantidad de radio transmisiones que puede efectuar el dispositivo. Este campo debe ser decrementado en 1 por cada dispositivo receptor que este enlazado.

Número de Secuencia: Está siempre presente y posee una longitud de 8 bits. Este campo debe ser incrementado en 1 por cada trama que sea transmitida; de esta forma, conjuntamente con la dirección de origen, sirven como un identificador de trama. Sin embargo, este campo representa una limitación al ser únicamente de 8 bits de longitud.

Dirección IEEE de Destino: Es un campo que si se encuentra presente posee una longitud de 64 bits. Esta dirección es a la que se le conoce como direccionamiento extendido y es correspondiente a la dirección de destino de 16 bits que se encuentra en el encabezado de esta capa. Si la dirección de destino es un broadcast, la dirección IEEE no debe estar presente.

Dirección IEEE de Origen: Posee 64 bits de longitud y está relacionado con la dirección de origen de 16 bits que se encuentra en el encabezado de la capa de red.

Control Multicast: Se encuentra presente solo sí en el campo de control de trama se especifica que se usara el envío multicast. Posee una longitud de 8 bits y permite especificar como se realizará la transmisión, esto es entre miembros de un grupo o desde un dispositivo que no es miembro hacia otros que pertenecen a un grupo

Subtrama de Ruta de Origen: Tiene una longitud de 8 bits de origen y solo puede estar presente si esta activado en el campo de Frame Control. Permite saber cual es el dispositivo más cercano al dispositivo de destino, en base a una bandera que posee que funciona manera de contador y otra que permite identificar al dispositivo

Payload: Depende si la trama es de datos o de comando, para el primer caso el payload representa toda la información que la capa superior requiere que esta capa transmita, mientras que cuando la trama es de comandos el payload contendrá el identificador del comando y el comando en sí. **[25]**

2.6.3. PDU de Capa MAC

Existen cuatro tipos de tramas MAC (MPDU), que constan de un encabezado, payload y una cola. Las tramas MAC que se encuentran dentro de la especificación IEEE 802.15.4 son de Beacon, Datos, ACK y de comandos. A continuación se presenta el formato de la MPDU general:

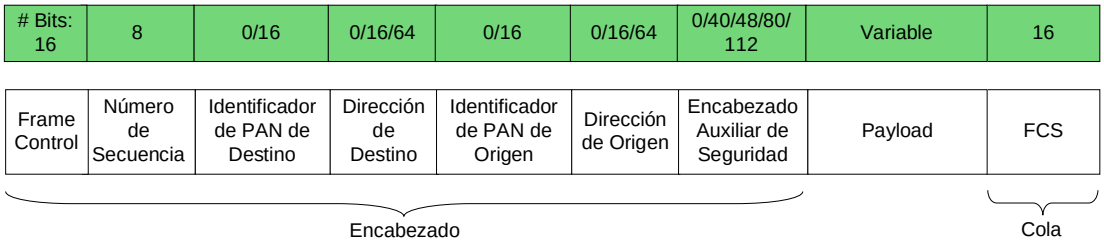


Figura. 2.12. Formato General de PDU de capa MAC (MPDU)

Frame Control: Tiene una longitud de 16 bits, distribuidos en subcampos o banderas que permiten establecer si la trama que se envía es de datos, beacon, ACK o de comandos. También permite determinar que tipo de direcciones se usaran, las cortas (16 bits) o las extendidas (64 bits), tanto para direcciones de origen como de destino. Otra bandera permite saber que versión del estándar se está utilizando.

Número de Secuencia: Tiene 8 bits de longitud y especifica el número de secuencia de la trama.

Identificador de PAN de Destino: es un campo de 16 bits que se encuentra presente únicamente si la bandera en el campo Frame Control indica que se usaran identificadores de PAN. Cuando este campo posee un valor de 0xffff, se

entiende un identificador de PAN valido para todos los dispositivos que se encuentren en el canal.

Dirección de Destino: Su longitud depende de las banderas en el campo Frame Control, ya que puede no estar presente en la trama, así como también puede usar el direccionamiento corto o extendido.

Identificador de PAN de Origen: Tiene las mismas consideraciones que el campo “Identificador de PAN de Destino”.

Dirección de Origen: Tiene las mismas consideraciones que el campo “Dirección de Destino”

Encabezado Auxiliar de Seguridad: Tiene una longitud variable que especifica la información requerida para el proceso de seguridad, como el nivel actual de seguridad que esta usando o el identificador de la clave que se encuentra en su tabla de datos

Payload: Tiene una longitud variable y viene desde las capas superiores. Si dentro del campo de Frame Control se especifica que la seguridad esté habilitada, el payload será protegido.

FCS (Frame Check Sequence): Posee una longitud de 16 bits que permite asegurar que la información enviada es la que se recibe. Para esto utiliza el algoritmo C*yclic Redundancy Check (*CRC), que comprueba los bits del encabezado y del payload, como resultado crea un número que ocupara los 16 bits. Cuando el receptor recibe una trama, también corre el algoritmo CRC, si el valor resultante es igual al que le envió el dispositivo transmisor en este campo, se toma como valida la trama, caso contrario se la descarta

2.6.4. PDU de la Capa Física

La PDU de la Capa Física (PPDU) consiste básicamente de tres componentes que son los campos de sincronización, el encabezado y el payload variable que contiene la información proveniente de la Capa MAC. El formato general de la PPDU es el siguiente:

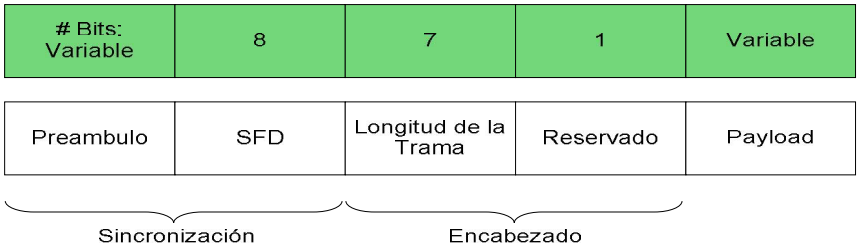


Figura. 2.13. Formato General de PDU de la Capa Física (PPDU)

Preámbulo: este campo es usado por el transceiver, para realizar la sincronización con los mensajes entrantes. Su longitud es variable y depende del tipo de modulación que utilice la Capa Física. De esta forma, se tiene la longitud del campo en base a la siguiente tabla:

Tabla. 2.6. Longitud del Campo Preámbulo

Capa Física	Longitud del Campo Preámbulo (Bits)
868–868.6 MHz BPSK	32
902–928 MHz BPSK	32
868–868.6 MHz ASK	40
902–928 MHz ASK	30
868–868.6 MHz O-QPSK	32
902–928 MHz O-QPSK	32
2400–2483.5 MHz O-QPSK	32

Delimitador de Inicio de Trama (*Star of Frame Delimiter*- SFD): Indica el fin del campo de sincronización y el inicio del encabezado del PPDU. Tiene una longitud de 8 bits.

Longitud de la Trama: Contiene 7 bits de longitud e indica la cantidad de octetos que tendrá el payload, es decir la información proveniente de las capas superiores. Este campo puede tomar el valor de 5, para indicar que es una trama ACK, o un valor comprendido entre 9 y 127 para cualquier otra trama MPDU.

Payload: Es de longitud variable y contiene la información proveniente de las capas superiores.

2.7. MODELO DE TRANSFERENCIA DE DATOS

Para realizar la transferencia de datos, la red puede funcionar con el envío de Beacons o sin el envío de ellos. Las tramas Beacon permiten realizar la sincronización de dispositivos enlazados, identificar a la PAN y determinar la estructura de la supertrama (*superframe*).

Dentro de las redes que usan beacons, la supertrama es una estructura que esta definida por el coordinador de red. Consta de 16 *time slots* de igual tamaño, de los cuales el primero es usado para enviar un beacon. Opcionalmente la supertrama puede agregar también un periodo inactivo, en la cual los dispositivos entran en modo de bajo consumo. A la porción activa también se la conoce como *Contention Access Period* (Período de Contención de Acceso, CAP), en el cual cada dispositivo que quiere comunicarse tratará de ganar un *time slot* mediante el mecanismo CSMA-CA.

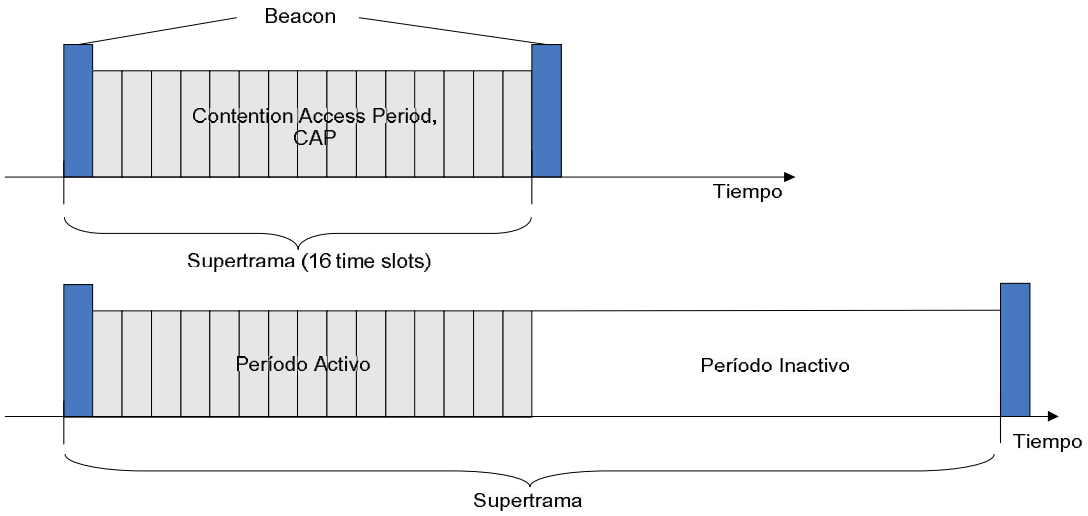


Figura. 2.14. Estructura de Supertrama sin período inactivo y con período inactivo

Cuando una determinada aplicación requiere baja latencia o un mayor ancho de banda, el coordinador de red agrupa ciertos *time slots* del final del CAP, en el llamado *Contention Free Period* (Período Libre de Contención, CFP), en el cual a cada slot se lo llama *Guaranteed Time Slot* (Espacio Garantizado de Tiempo, GTS). El coordinador se encargará de asignar uno o más GTS a la aplicación que lo necesite, garantizando que dentro de cada supertrama pueda realizar la transmisión de información, sin competir con los otros dispositivos de la red.

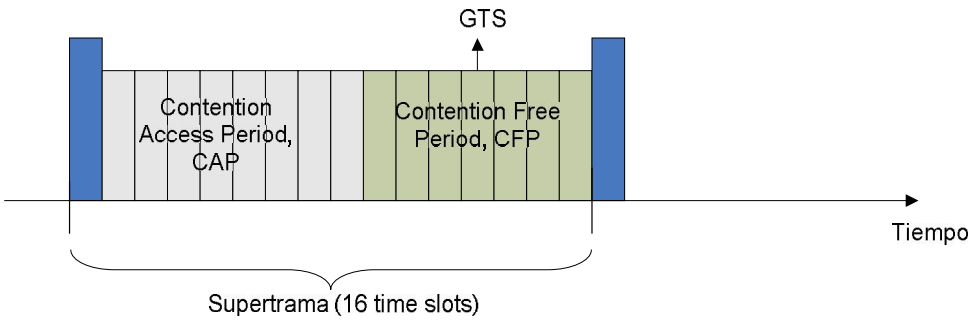


Figura. 2.15. Supertrama con uso de GTS (Guaranteed Time Slot)

La transferencia de datos puede ser de tres tipos: desde un dispositivo hacia un coordinador, desde el coordinador hacia un dispositivo y la transferencia de datos entre dos dispositivos directamente. Cada uno de estos modelos es diferente para el caso en que la red utilice o no el envío de Beacons.

2.7.1. Transferencia de Datos hacia un Coordinador ZigBee

En una red con beacon activado, el dispositivo primero busca al beacon, una vez que lo ha encontrado se sincroniza al modelo de supertrama que se este usando. Posteriormente, mediante el mecanismo CSMA-CA para ganar un *time slot,* podrá realizar la transmisión de datos. Cuando el coordinador ha recibido los datos, y sí se encuentra especificado dentro de las opciones de la PAN, se enviará una trama de ACK (*acknowlegment)* para confirmar la llegada.

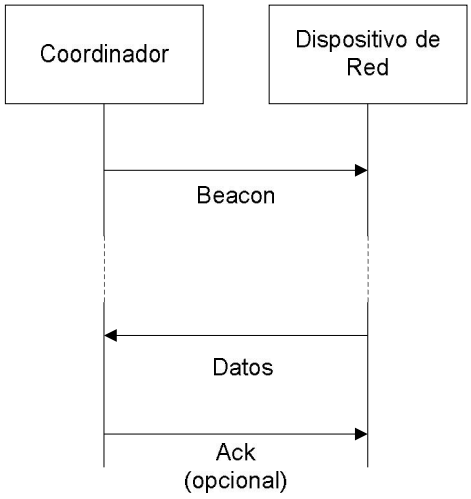


Figura. 2.16. Transferencia de Datos hacia el Coordinador ZigBee en una PAN con Beacon

En una PAN que no utiliza Beacon, la transmisión es más simple. La trama de datos se envía a través del canal mediante el mecanismo CSMA-CA, hacia el coordinador. De igual forma, al recibirse la trama, es opcional el envío de un ACK para confirmar la llegada.

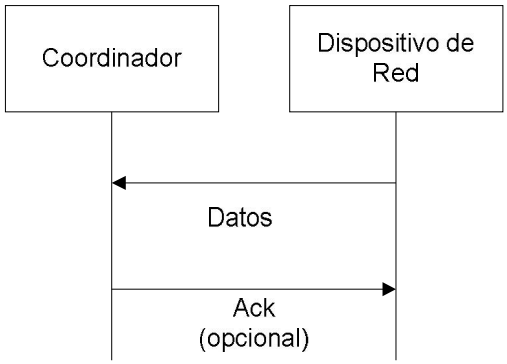


Figura. 2.17. Transferencia de Datos hacia el Coordinador ZigBee en una PAN sin Beacon

2.7.2. Transferencia de Datos desde un Coordinador ZigBee

Dentro de una PAN que utiliza beacon, cuando un coordinador ZigBee desea enviar ciertos datos, lo hace mediante el beacon, indicando que existen datos pendientes de ser enviados. Los dispositivos de la red se encuentran constantemente escuchando el beacon y cuando encuentran uno que les indica que tienen un mensaje pendiente para ellos, generan una trama de comandos a nivel de capa MAC para solicitar el envío de los datos. El coordinador se encarga de enviar una trama ACK indicando que ha llegado su petición (*data request*) y a continuación envía las trama de datos. Una vez recibida los datos, el dispositivo de red puede opcionalmente enviar un ACK para confirmar su llegada. Para finalizar este proceso, se remueve el mensaje de datos pendientes del beacon de la PAN. Todos estas tramas se envían utilizando el mecanismo CSMA-CA para ganar un *time slot* vacío.

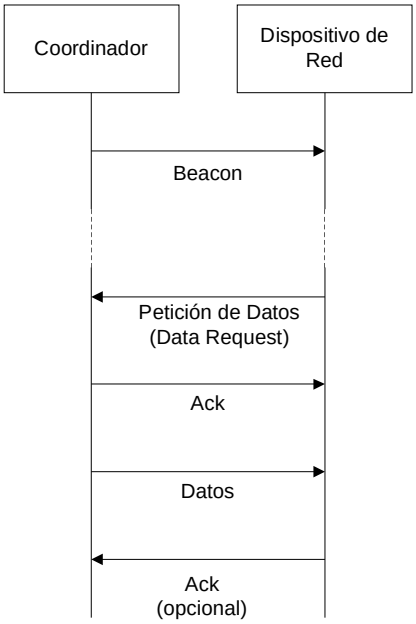


Figura. 2.18. Transferencia de Datos desde un Coordinador ZigBee en PAN con Beacon

En una red sin Beacon, el Coordinador se encarga de almacenar la trama de datos y espera a que el dispositivo de red le envíe una petición (*data request*), esto en base a lo que se encuentre definido en alguna aplicación que maneje el dispositivo. Cuando el Coordinador recibe esta petición envía como respuesta una trama ACK. Si existe algún mensaje para el Dispositivo de Red que lo solicitó se lo envía a continuación; pero si no hay una trama de datos pendiente, puede notificarlo directamente en el ACK que envía después del *Data Request* o puede enviar una trama de datos con un payload de longitud de cero bits. Cuando el Dispositivo Final recibe la trama de datos envía un ACK para confirmar su llegada.

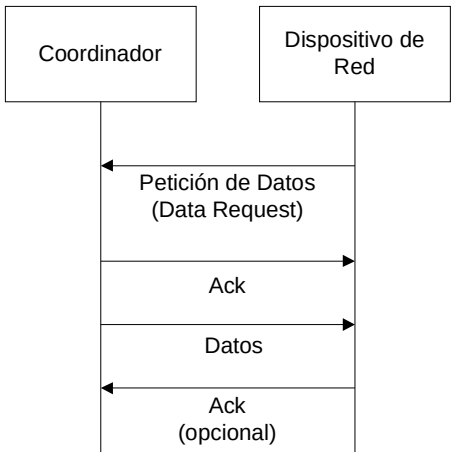


Figura. 2. 19. Transferencia de Datos desde un Coordinador ZigBee en PAN sin Beacon

2.7.3. Transferencia de Datos entre Dispositivos de Red

En una PAN *Peer-to-Peer*, cada dispositivo puede comunicarse con cualquier otro dispositivo de la red dentro de su rango de influencia. Para lograr la comunicación de datos lo puede hacer ya sea enviando directamente las tramas o sincronizándose primero con el dispositivo. Para los dos casos utiliza el método CSMA-CA para asegurarse que otros dispositivos no estén enviando al mismo tiempo otras tramas al mismo dispositivo.

CAPÍTULO 3

CONCEPTOS BÁSICOS SOBRE NETWORK SIMULATOR 2.32

2.8. INTRODUCCIÓN

Network Simulator es uno de los programas más utilizados actualmente para el desarrollo de simulaciones referentes a redes, tanto cableadas como inalámbricas, gracias a que su distribución es libre y sus bloques de códigos y librerías pre-existentes son modificables de acuerdo a las necesidades de los usuarios.

El simulador surgió como parte del proyecto VINT (*Virtual InterNetwork Testbed*), con el apoyo y la colaboración de la Universidad de California del Sur con su Instituto de Ciencias de la Información (USC/ISI) y la Universidad Berkeley de California con su Laboratorio Nacional Lawrence Berkeley (LBNL). El objetivo del proyecto era desarrollar un software que permita la simulación de entornos de red para conocer la manera de interactuar de los diferentes protocolos de Internet. **[26]**

NS-2 es un simulador de eventos y cuyo lenguaje de programación está orientado a objetos. Los tipos de lenguajes que usa son C++ y OTcl, dependiendo si se requiere realizar una corrida rápida o realizar modificaciones rápidas. Los dos lenguajes son perfectamente compatibles, y mediante estructuras internas del software las variables definidas en C++ se pueden usar en OTcl y viceversa.

De tal forma que C++ se usa frecuentemente para implementar protocolos de manera detallada variando sus parámetros, ya que la corrida es rápida y se maneja a nivel de bits o encabezados pero los cambios son más laboriosos de realizar. Mientras que OTcl es un lenguaje más fácil de interpretar por lo que los cambios son más rápidos, pero la compilación es más lenta, por lo que se usa principalmente para desarrollar los escenarios.

Las simulaciones en NS-2 permiten implementar varios protocolos, ya sean de transporte o de enrutamiento. También permiten definir y generar topologías simples o complejas. Dentro de las simulaciones es necesario crear y asociar a cada nodo un agente que es el encargado de generar o recibir un paquete. Los tipos de tráfico que se pueden manejar incluyen simulaciones de aplicaciones FTP, Telnet y Web.

2.9. MÓDULOS DE NS-2 [27][28]

Los módulos que contienen el simulador NS-2, sirven para poder desarrollar los escenarios, configurar los protocolos y obtener resultados para poder analizarlos o visualizarlos.

Mediante el siguiente gráfico se puede comprender como se encuentra estructurado el Simulador NS-2.

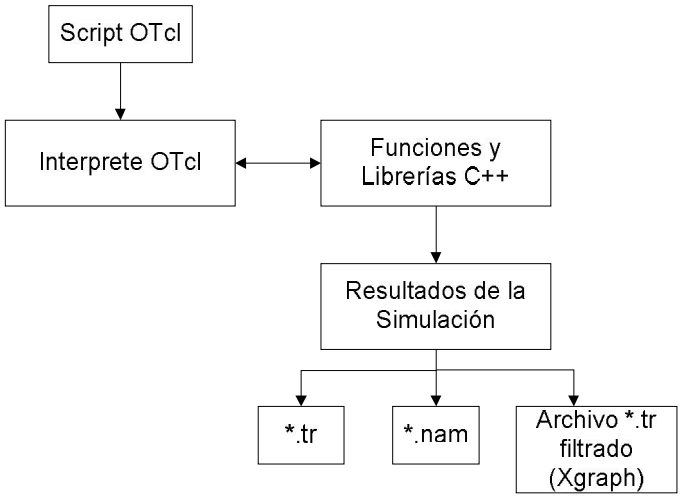


Figura. 3.1. Esquema del Simulador NS-2

2.9.1. Script OTcl

Contiene toda la información necesaria para desarrollar la simulación en NS-2, ya que permite especificar todos los elementos que participan en el escenario de simulación como son los nodos, el tipo de enlace que se usará, el tipo de tráfico que se intercambiara, la topología de red, además construye los agentes que son los encargados de generar o recibir los paquetes.

Dentro del *script* se encuentra especificada la creación de los archivos de traza o de los archivos que permiten correr la simulación gráfica; además, mediante líneas de comandos se establece el tiempo de inicio de un evento, que es el encargado de desencadenar la simulación.

El script está elaborado utilizando lenguaje OTcl, por lo que la extensión de este archivo es *.tcl. Para abrir un script se utiliza la línea de comando *ns nombre_scrip.tcl.*

2.9.2. Interprete OTcl y Librerías C++

El interprete OTcl permite analizar línea por línea el script que se crea anteriormente para desarrollar la simulación, por motivos de velocidad de procesamiento en C++ existen librerías que OTcl no maneja y que gracias a la dualidad que existe entre los dos lenguajes, pueden ser llamadas y procesadas.

2.9.3. **Traza de Salida de la Simulación [29]**

Uno de los archivos de salida que se puede obtener de la simulación es el llamado traza con extensión *.tr, que registra los eventos que se desarrollaron en la red.

Este tipo de archivo es una especie de tabla de datos con varias columnas, que principalmente indican cada evento de recepción o envío de paquetes y

desde que nodo y hacia que nodo se realizó. La estructura general de un archivo de traza es la siguiente:

Evento	Tiempo	Nodo Origen	Nodo Destino	Tipo de Paquete	Tamaño del Paquete	Flags	ID de Flujo	Dirección de origen	Dirección de destino	Número de Secuencia	ID del Paquete

Figura. 3.2. Estructura General de un archivo de Traza

```
1     2      3   4   5   6      7   8   9      10  11  12
↓     ↓      ↓   ↓   ↓   ↓      ↓   ↓   ↓      ↓   ↓   ↓
r 17.922645 201 202 tcp 552 ------- 0 10.47 191.17 28 49925
+ 17.922645 202 203 tcp 552 ------- 0 10.47 191.17 28 49925
d 17.922645 202 203 tcp 552 ------- 0 10.47 191.17 28 49925
r 17.922648 203 199 udp 200 ------- 0 204.0 199.60 3143 49809
r 17.922744 203 202 ack 40 ------- 0 191.12 10.42 394 49934
+ 17.922744 202 201 ack 40 ------- 0 191.12 10.42 394 49934
- 17.922744 202 201 ack 40 ------- 0 191.12 10.42 394 49934
- 17.922913 202 203 ack 40 ------- 0 133.90 180.10 72 49904
r 17.922968 203 199 udp 200 ------- 0 204.0 199.60 3144 49813
```

Figura. 3.3. Muestra de Archivo de Traza

1.- El evento puede ser considerado de cuatro tipos para redes cableadas: ***r*** (recibido en el extremo del link), **+** (enqueued o puesto en cola), **-** (dequeued o sacado de la cola) y ***d*** (dropped o desechados). Mientras que para redes inalambricas los eventos son: **r**(recibido),**s** (enviado), **f** (forward, transmitido) y **d** (dropped)

2.- Representa el tiempo en que ocurre el evento

3.- Es el nodo al inicio del enlace en el cual ocurre el evento

4.- Es el nodo al otro extremo del enlace en el cual ocurre el evento

5.- Corresponde al tipo de paquete que puede ser por ejemplo TCP, CRB, UDP, ACK , entre otros que se seleccionan en el script de entrada.

6.- El tamaño del paquete en bytes.

7.- Algunas banderas, pero que no son muy usadas y pueden no constar

8.- El identificador de flujo es definido para Ipv6, por lo que se lo usará en el futuro para análisis

9.- Es la dirección origen que maneja internamente el simulador

10.- Es la dirección destino manejada de igual manera que el anterior campo

11.- Corresponde al identificador de secuencia de paquetes de la capa de red. Aun cuando UDP no utiliza número de secuencia, este campo siempre tiene un valor para fines de análisis por parte del simulador

12.- Indica el identificador único de paquete

2.9.4. **Visualizador gráfico NAM [30] [31]**

Network Animador (NAM), es una aplicación externa al simulador NS-2.32, pero que viene incluido en el paquete completo. Esta herramienta esta basada en el lenguaje Tcl y se encarga de mostrar de manera gráfica los escenarios de simulación.

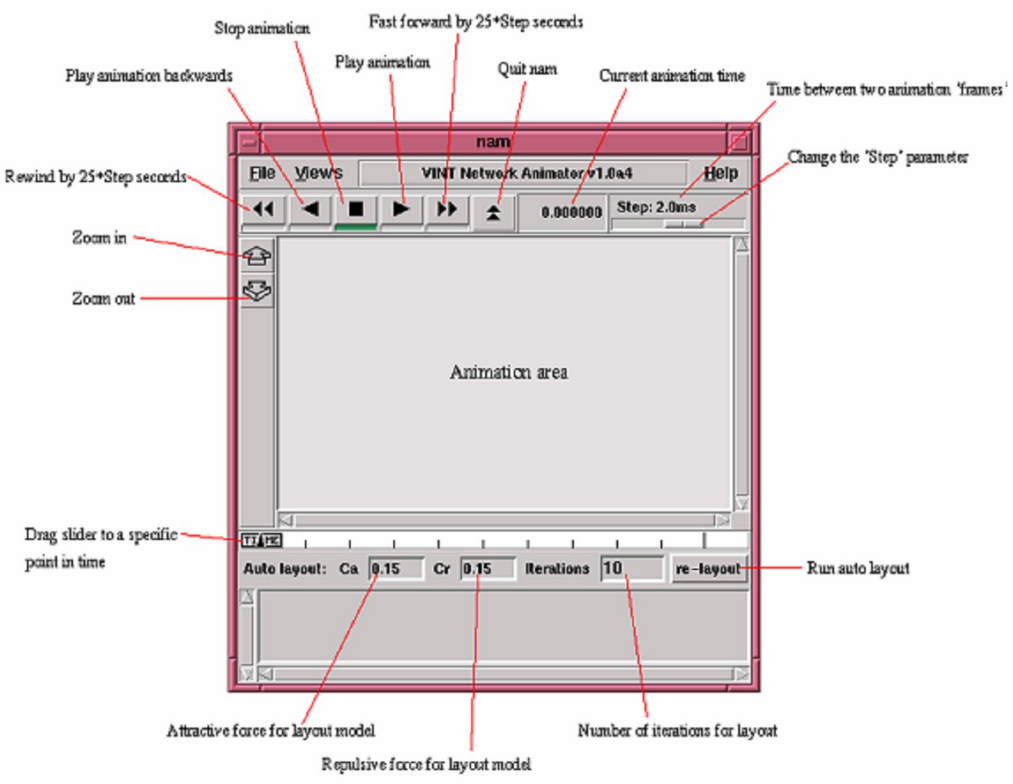


Figura. 3.4. Interfaz gráfica del NAM

Gracias a la interfaz que se puede apreciar en la figura 3.4., es posible realizar adelantos o retrocesos en el tiempo de simulación para poder observer que es lo que ocurre en cada evento que se programó. Todo esto debido a que la visualización no esta ocurriendo en tiempo real, todos los datos necesario ya fueron procesados y almacenados en un fichero con extensión *.nam. Para abrir el archivo que se genera al finalizar la simulación se utiliza el comando *nam <nombre_fichero>.nam* desde el prompt general.

Con el NAM es posible visualizar los siguientes elemendos que intervienen en la simulación:

a) Nodos con su respectiva numeración

b) Elnaces entre los nodos para redes cableadas o rangos de cobertura para redes inalámbricas

c) Flujo de información que cruza entre cada nodo de la red

d) Colas de paquetes que se formanan en cada nodo

e) Envío y caidas de paquetes

f) Caidas y levantamientos de enlaces para redes cableadas

En la figura 3.5. se puede ver como se encuentra la cola de paquetes en el nodo 2 y como se envían paquetes UDP en azul y TCP en rojo. En la figura 3.6 se aprecia una red inalámbrica en la que cada circulo alrededor del nodo representa el rango de cobertura.

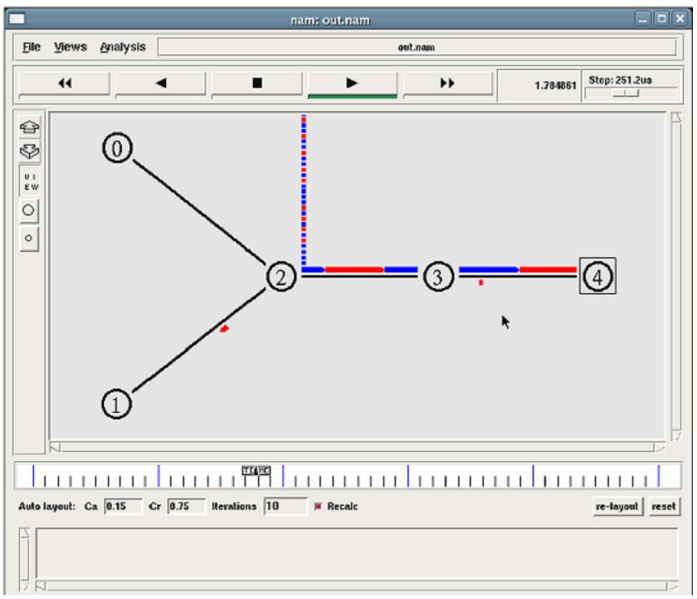


Figura. 3.5. Ejemplo de NAM para una red cableada

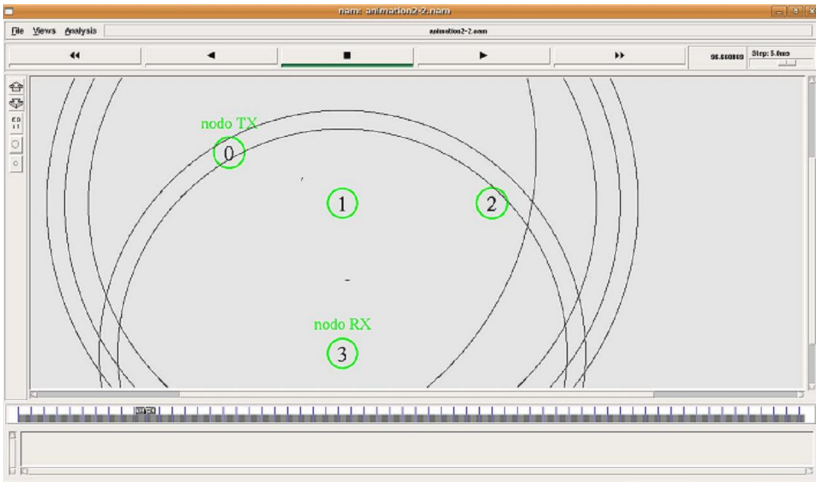


Figura. 3.6. Ejemplo de NAM para una red inalámbrica

2.9.5. **XGRAPH [32]**

También es una aplicación externa a Network Simulator, pero que viene incluida en el paquete completo de instalación NS-2.32. Esta aplicación nos permite visualizar gráficos de curvas, correspondientes a un archivo de traza con formato de columnas x y.

Para obtener el archivo de traza en el formato *x-y*, se puede hacer uso de varios métodos entre los que se tiene los siguientes:

- Creación y ejecución de un pequeño script PERL (*Practical Extraction and Report Language*), cuyo principla uso es la busqueda, extracción y reporte de determinados caracteres. Este lenguaje interpretativo puede ser ejecutado en varios sistemas operativos sin cambiar su código, por lo que es muy usado para realizar filtros de archivos.

  Para poder ingresar una traza al Xgraph, el script nos debe permitir extraer un archivo en el cual conste por ejemplo los paquetes TCP enviados entre los nodos en un determinado tiempo, de esta forma, se genera un nuevo archivo de traza con unicamente la información del instante en que se realizó

el envió del paquete TCP, pudiendo de esta forma generar un gráfico en formato *x – y*.

- Uso de los comandos awk y grep, mediante los cuales tambien se puede filtrar los archivos de traza para obtener el formato requerido para ser usado en Xgraph; sin embrago, no llegan a ser tan específicos como se lograría con un script perl. La ventaja de estos comandos es que no necesitan de una corrida, por lo que se los puede incluir en el script de simulación o ejecutar el comando en el promp general, tomando como archivo de origen el archivo de traza que genera la simulación previa.

Una vez que ya se tiene el archivo de traza filtrado y en formato x – y, se ejecuta el comando xgraph en el pormp general llamando a dicho archivo. Algunos indicadores que se le puede adicionar al grafico son los siguientes:

- Titulo: usando el comando **–t *"titulo"***

- Tamaño del gráfico: con el comand **–geometry *tamaño_x tamaño_y***

- Titulo de los ejes: mediante **–x "*titulo_x*" –y "*titulo_y*"**

Por ejemplo si tenemos el archivo ya filtrado que se llama salida1.tr y que correspodne a la tasa de paquetes perdidos, la manera de ejecutar el xgraph sería la siguiente: *xgraph* salida *–geometry 800x400 –t "Tasa de perdidas" –x "Tiempo" –y "Paquetes Perdidos"*

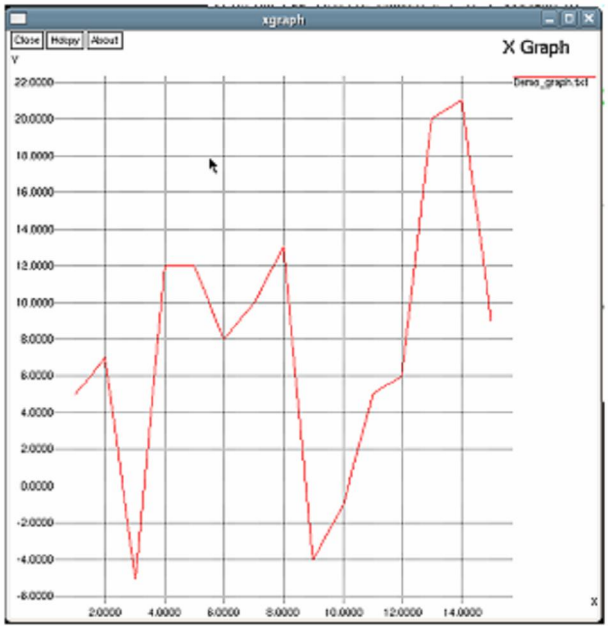


Figura. 3.7. Ejemplo de ventana de visualización de aplicación Xgraph

2.10.MODELOS DE PROPAGACIÓN EN NS-2 [33]

El Simulador NS2.32 tiene la opción de manejar diferentes modelos de propagación, que le permiten determinar el nivel de energía o potencia con el que es recibida la señal de un paquete en la capa física del receptor inalámbrico.

Dentro del simulador cada capa física de los diferentes nodos inalámbricos tiene una variable que corresponde al umbral de energía con el que debe ser recibida una señal. Se considera que la transmisión no fue exitosa cuando la señal posee una potencia por debajo del valor de dicho umbral, entonces la capa física envía esta información a la capa MAC y esta se encarga de reportar un error y de descartar el paquete.

Existen tres modelos de propagación que puede implementar el NS2.32 y son los siguientes:

- *Free Space*
- *Two-Ray Ground Reflection*
- *Shadowing*

2.10.1. **Modelo de Propagación *Free Space***

Este modelo de propagación es usado cuando se requiere simular un canal inalámbrico de comunicación con un camino directo y con línea de vista entre el trasmisor y el receptor.

La ecuación para calcular la potencia de la señal en espacio libre a una distancia *d* es la siguiente:

$$P_r(d) = \frac{P_t \times G_t \times G_r \times \lambda^2}{(4\pi)^2 \times d^2 \times L}$$

Donde:

$P_r(d)$ = Potencia recibida en función de distancia *d*
P_t = Potencia transmitida
G_t = Ganancia de la antena del trasmisor
G_r = Ganancia de la antena del receptor
λ = Longitud de onda
d = Distancia
L = Factor de Pérdidas por propagación

De manera general el simulador asume para este modelo G_t=G_r=1, y *L*=1. Este modelo representa el rango de comunicación como un círculo alrededor del

trasmisor, sí el receptor se encuentra dentro de este círculo los paquetes llegarán con éxito, caso contrario serán descartados.

El comando OTcl para utilizar este modelo está dentro de *node-config* y es:

$ns_ node-config -propType Propagation/FreeSpace

Otra manera forma de usarlo es mediante:

set prop [new Propagation/FreeSpace]
$ns_ node-config -propInstance $prop

2.10.2. **Modelo *Two-Ray Ground Reflection***

Este modelo es mucho más realista que el modelo *Free Space,* ya que en la práctica la mayoría de ocasiones existen más de dos caminos entre el receptor y el transmisor. De tal forma, el modelo de dos rayos, considera que existe línea de vista directa entre el trasmisor y receptor, pero además considera la posible reflexión de la señal en la tierra.

El modelo de dos rayos es más exacto que el de espacio libre, para mayores distancias, la ecuación para el cálculo de la potencia recibida a una distancia *d* es la siguiente:

$$P_r(d) = \frac{P_t \times G_t \times G_r \times h_t^{\,2} \times h_r^{\,2}}{d^4 \times L}$$

Donde:

h_t= altura de la antena del trasmisor
h_r= altura de la antena del receptor

El modelo de dos rayos no es útil para distancias cortas ya que las oscilaciones contractivas y destructivas de las ondas directa y reflejada causan errores. Por este caso se debe usar el modelo de Espacio Libre.

El comando Otcl para utilizar este modelo es:

$ns_ node-config -propType Propagation/TwoRayGround

O como otra alternativa:

set prop [new Propagation/TwoRayGround]
$ns_ node-config -propInstance $prop

2.10.3. Modelo de Propagación *Shadowing*

Tanto el modelo *Free Space* como de Dos Rayos visualizan de manera idealista el rango de cobertura como un círculo, esto debido a que su predicción de la potencia recibida está basada en una función determinística de la distancia; es decir entregan un valor promedio de la potencia a una determinada distancia; pero en realidad la potencia recibida es una variable aleatoria debido a los múltiples trayectos que puede darse al momento de la propagación de la señal.

El modelo *Shadowing* consta de dos cálculos, el primero es el cálculo de las perdidas por el trayecto (*Path Loss*), que también equivale a predecir la potencia media recibida a una distancia *d*, además calcula la potencia media a una distancia referencial *do* para relacionarlas. Para expresarla en dB la fórmula quedaría de la siguiente manera:

$$\left[\frac{P_r(d)}{P_r(d_0)}\right]_{dB} = -10\beta \log\left(\frac{d}{d_0}\right)$$

Donde β representa el exponente de perdidas por trayecto (path loss exponent) y se obtiene de la siguiente tabla:

Tabla. 3.1. Valores Típicos de β

Environment		β
Outdoor	Free Space	2
	Shadowing urban area	2,7 to 5
In building	line of sight	1,6 to 1,8
	Obstructed	4 to 6

La segunda parte del modelo *Shadowing* refleja la variación de la potencia a una determinada distancia, mediante una distribución Gaussiana expresada en dB, que posee una media igual a cero y una desviación σ en dB, llamada desviación shadowing que se obtiene de la siguiente tabla:

Tabla. 3.2. Valores Típicos de σ dB

Environment	σ_{dB} (dB)
Outdoor	4 to 12
Office, hard partition	7
Office, soft partition	9,6
Factory, line of sight	3 to 6
Factory, obstructed	6,8

Finalmente la ecuación quedaría de la siguiente manera:

$$\left[\frac{P_r(d)}{P_r(d_0)}\right]_{dB} = -10\beta \log\left(\frac{d}{d_0}\right) + X_{dB}$$

De esta manera se cambia la idea de que el rango de cobertura es un círculo por un modelo probabilístico.

Los comandos OTcl están dentro de la interfaz node-config de la siguiente manera:

```
Propagation/Shadowing set pathlossExp_ 2.0  ;# β
Propagation/Shadowing set std_db_ 4.0       ;# σ (db)
Propagation/Shadowing set dist0_ 1.0        ;# distancia de referencia (m)
Propagation/Shadowing set seed_ 0           ;# seed para RNG (Generador
                                            ;de Número Randómico

$ns_ node-config -propType Propagation/Shadowing
```

2.11.PROTOCOLOS DE ENRUTAMIENTO EN NS-2 [34][35][36]

Un protocolo de enrutamiento es el encargado de determinar por cual ruta se enviarán los paquetes de un nodo hacia otro, basándose en un esquema de la topología de red que mantienen gracias a diferentes condiciones del enlace que analizan; como pueden ser el ancho de banda, el número de saltos, la calidad del enlace, etc.

El protocolo de enrutamiento se encuentra configurado únicamente en dispositivos con capacidad de enrutamiento; es decir, dentro de las WPAN solo se encuentran establecidos en los FFD (*Full Funtion Device)*, ya sea que actúen como coordinador de red o como router.

Tanto las redes cableadas como las inalámbricas poseen sus propios protocolos de enrutamiento, esto debido a que son dos estructuras con requerimientos distintos. Algunos de los motivos que llevaron a crear protocolos de enrutamiento específicos para redes inalámbricas y alámbricas son los siguientes:

- En las redes cableadas los nodos son fijos y se asocia su ubicación con una dirección de red, pero en las redes inalámbricas los nodos son móviles, por lo que los prefijos de red no son válidos y la escalabilidad de la red resulta ser un problema

- Las redes inalámbricas poseen nodos que pueden entrar en modo de ahorro de energía, ante lo cual los protocolos de redes cableadas observarían nodos que aparecen y desaparecen, generando una gran cantidad de mensajes de control y consumiendo un gran ancho de banda

- El consumo de batería es de suma importancia en redes inalámbricas, por lo que los protocolos de enrutamiento para este tipo de redes deben optimizar este recurso y no mal utilizarlo al calcular nuevamente toda una ruta o enviar mensajes de vecindad continuamente como sucede con algunos protocolos de redes cableadas

- Los protocolos de enrutamiento en redes inalámbricas deben poseer un mejor control de *bucles,* ya que al existir rutas que no están limitadas por la existencia de un cable, sino mas bien por rangos de coberturas, los paquetes que no encuentran su destino pueden permanecer indefinidamente en la red consumiendo recursos de los enlaces

- El algoritmo y el tiempo de procesamiento para calcular la ruta, no deben exigir un gran consumo de energía en los nodos de redes inalámbricas

2.11.1. Clasificación de los protocolos de enrutamiento para redes MANET

Existen varios criterios para clasificar a los protocolos de enrutamiento para redes inalámbricas que poseen nodos móviles, pero la mas general los divide en proactivos y reactivos, dependiendo de si mantienen tablas o no para realizar el enrutamiento. Las características de estos protocolos son las siguientes:

- **Proactivos o basados en tablas:** Fueron los primeros protocolos que se crearon para redes Ad-Hoc, y actualmente se los considera poco eficientes, ya que se encargan de mantener constantemente actualizadas las rutas hacia todos los nodos de la red, consumiendo de esta forma gran parte del ancho de banda de los enlaces. Estos protocolos constantemente se encuentran generando tablas de enrutamiento que son transmitidas a los otros nodos, esto debido a que los nodos constantemente aparecen y desaparecen.

  Los protocolos preactivos difieren entre sí por el número de tablas de enrutamiento que requieren o por la manera en que difunden los cambios en la topología, así como también que datos se encuentran dentro de dichas tablas

  Estos protocolos se suelen usar especialmente cuando se requiere que la latencia de los paquetes sea muy baja o cuando la tasa de movilidad de los nodos es muy alta. Los principales protocolos preactivos son: DSDV (*Destination- Sequenced Distance-Vector Routing Protocol*), CGSR (*Clusterhead Gateway Switch Routing*), WRP (*Wireless Routing Protocol*), OLSR (*Optimized Link State Routing*) y TBRPF (*Topology Dissemination Based on Reverse-Path Forwarding*).

- **Reactivos o bajo demanda:** estos protocolos no intentan conocer todas las rutas, solo las buscan cuando necesitan enviar un paquete, lo que representa un menor gasto del ancho de banda del enlace

  La latencia del primer paquete que se envía hacia el mismo destino es mucho mayor que para el resto de paquetes, esto obviamente debido a que primero necesita buscar la ruta, mientras que para los siguientes paquetes la ruta ya está establecida. Los caminos de enrutamiento una vez que han sido encontrados se mantienen para su uso, pero debido a que la red esta en movimiento, después de un cierto tiempo se las desechan.

Los protocolos mas relevantes son: AODV (*Ad Hoc On-Demand Distance Vector Routing*), DSR (*Dynamic Source Routing*), LQSR (*Link Quality Source Routing protocol*), LMR (*Lightweight Mobile Routing*) y TORA (*Temporary Ordered Routing Algorithm*).

Otro tipo de clasificación los separa en protocolos de enrutamiento de salto a salto o protocolos de origen.

- **Protocolos de enrutamiento Salto a Salto:** El encaminamiento se da cuando cada nodo determina el siguiente salto al que será enviado el paquete.

- **Protocolo de enrutamiento de origen:** el encaminamiento de origen se produce cuando el nodo que genera el paquete determina la ruta completa para alcanzar el destino, esta información se envía dentro del mismo paquete, ante lo cual los nodos intermediarios prácticamente no realizan ninguna actividad de ruteo, pero el volumen del paquete se ve claramente incrementado. El protocolo mas usado dentro de este tipo es DSR

También se los puede clasificar entre geográficos y no geográficos

- **Protocolos de enrutamiento Geográficos:** tienen en cuenta la posición geográfica exacta de cada nodo para poder determinar la ruta; sin embargo, y como desventaja se requiere que cada nodo disponga de dispositivos de posicionamiento global (GPS), pero esto incrementa su costo. Un ejemplo de este tipo de protocolos es *DREAM (Distance Routing Effect Algorithm for Mobility)*

Otra clasificación se basa en las diferentes jerarquías que puede tener un nodo dentro de la red:

- **Protocolos de Enrutamiento Jerárquicos:** Con estos protocolos los nodos tienen una jerarquía dentro de la red, mediante la cual se les permitirá retransmitir o no los mensajes que le lleguen. Los nodos son agrupados en bloques o *clusters*, en donde se asigna un ID a cada nodo, y alguno de ellos será la cabeza del cluster, que también servirá como *gateway* para comunicarse con grupos vecinos en la red. Un protocolo que maneja este tipo de enrutamiento es CGSR

- **Protocolos de Enrutamiento Plano:** Para estos protocolos, todos los nodos se encuentran en el mismo nivel y tienen las mismas funciones y responsabilidades.

Existe otra forma de clasificarlos en función de cuantas rutas mantienen los protocolos hacia cada destino, de esta manera se tiene:

- **Protocolos de Enrutamiento *Multipath* y *Singlepath:*** En donde *Tora*, es un ejemplo de protocolo de enrutamiento multipath ya que mantiene varias posibles rutas hacia los nodos de la red.

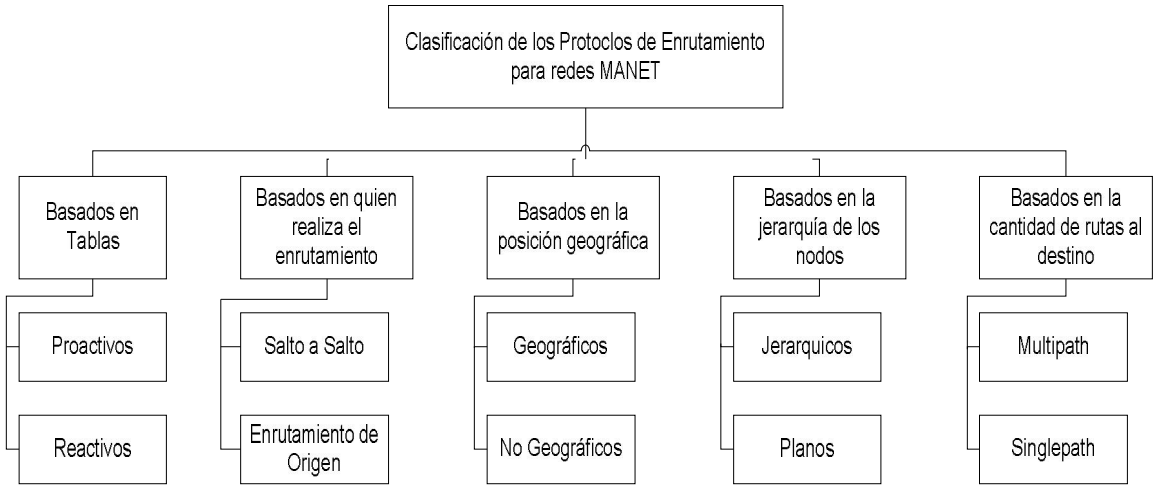


Figura. 3.8. Clasificación de los protocolos de enrutamiento para redes MANET

De todos los posibles protocolos de enrutamiento que se pueden usar en redes inalámbricas el Simulador NS-2.32 puede implementar únicamente los siguientes:

- DSDV
- AODV
- DSR

2.11.2. Protocolo de enrutamiento DSDV (*Destination - Sequenced Distance-Vector Routing Protocol)*

El protocolo de vector distancia de destino secuencial, está basado en el algoritmo que utiliza el protocolo de enrutamiento RIP para redes cableadas, en el cual se intercambia periódicamente toda la tabla de enrutamiento entre los nodos vecinos para estimar la distancia hacia cada uno de ellos.

La variación que introduce DSDV para que pueda funcionar en redes inalámbricas con nodos móviles, es que únicamente selecciona una ruta que la considera la más corta en relación al número de saltos.

Todas las rutas hacia los nodos destino están libres de bucles, gracias a que se introducen números de secuencia a cada ruta en cada actualización, de esta forma la ruta con mayor número de secuencia será la que se analice para determinar como llegar al destino, ya que se la considera la más reciente que se recibió.

Actualización de Rutas: se envía la tabla de rutas hacia los nodos vecinos mediante un broadcast periódicamente, sin embargo también se puede enviar actualizaciones cuando se detecta un evento, es decir puede existir un cambio de topología, la caída de un enlace, el ingreso o salida de un nodo, etc. La tabla de rutas posee varios campos pero los más relevantes son los siguientes:

- Nodo destino
- Siguiente Salto
- Métrica (número de saltos)
- Número de Secuencia del Destino

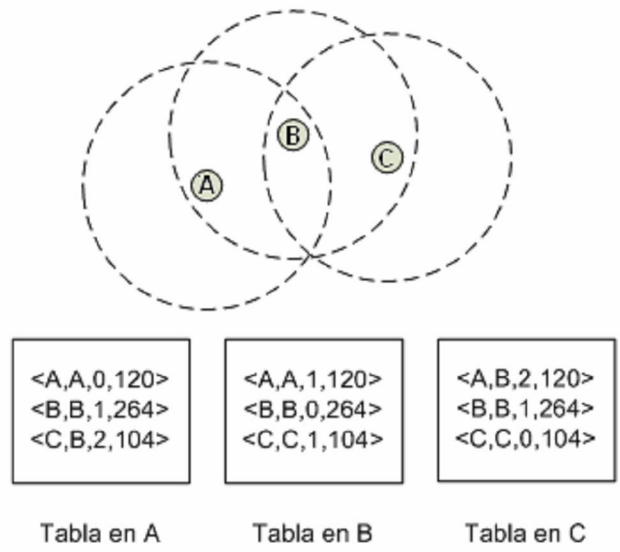


Figura. 3.9. Tablas que mantienen los nodos mediante el protocolo DSDV

Para el envío periódico de la tabla existen dos tipos de paquetes que puede utilizar DSDV, el que se transmite cuando existe un gran cambio en la red llamado *Full Dump,* el cual consta de toda la tabla de rutas; y un paquete de pequeña longitud llamado *incremental*, que transporta únicamente los cambios que se detectaron desde la última actualización.

Cuando existe un cambio en la ruta, el nodo que detecto dicho cambio lo transmitirá mediante una actualización, para lo cual incrementa su número de secuencia, de esa forma los otros nodos sabrán que esa ruta, al ser más nueva, es la que deben agregar a su tabla y reemplazar la anterior. Para realizara el incremento del número de secuencia se adiciona dos unidades al valor anterior que tenía dicho campo.

En la Figura 3.10 y 3.11 se puede ver como el nodo D, que ingresa a la red, envía un broadcast (con su tabla <D,D,0,2>) que le llegará a C por estar dentro de su rango de cobertura. Al detectar este cambio, C incluye esta ruta en su tabla,

incrementa su número de secuencia (de 104 a 106) y envía la actualización a los demás nodos. Como esta actualización tiene un número mayor de secuencia de C, los nodos la actualizan y también agregan la ruta D que se esta enviando.

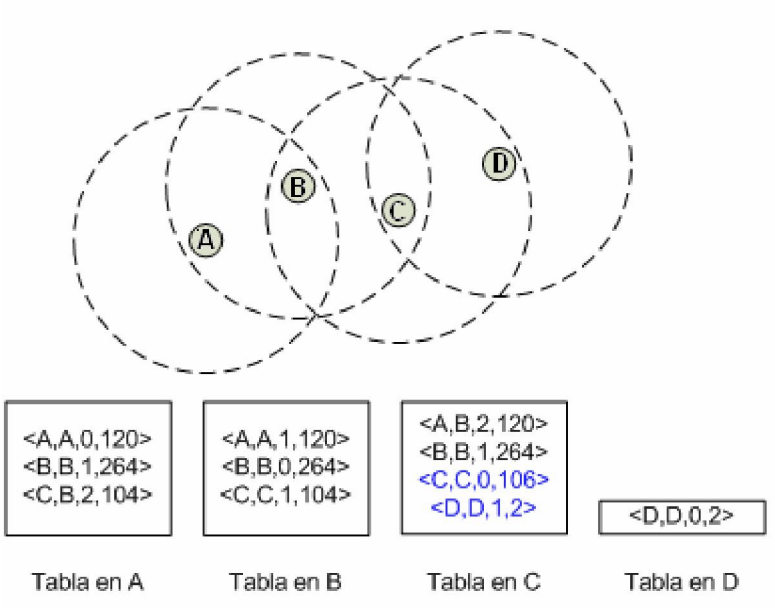


Figura. 3.10. Ingreso de un nodo cuando se usa el protocolo DSDV

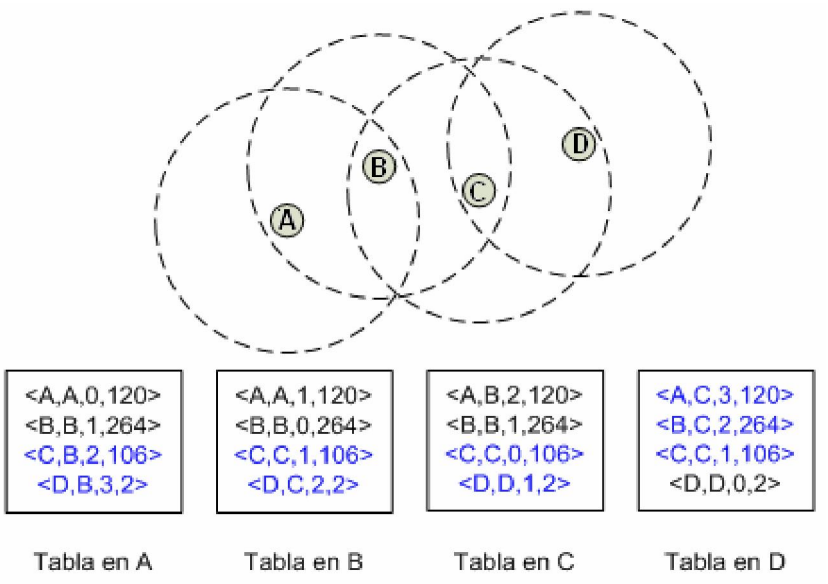


Figura. 3.11. Actualización de las tablas de rutas cuando se detecto un nuevo nodo con DSDV

Sí un nodo detecta que un enlace se ha caído, incrementa su número de secuencia en una unidad y coloca el valor de la métrica en 8, de esta manera la ruta se convierte en inalcanzable y será desechada por los otros nodos después de realizar la actualización de la tabla de rutas. Por ejemplo si tenemos la red de la Figura 3.11 que ya ha convergido, pero por algún motivo el nodo D abandona la red, se producirá el siguiente proceso:

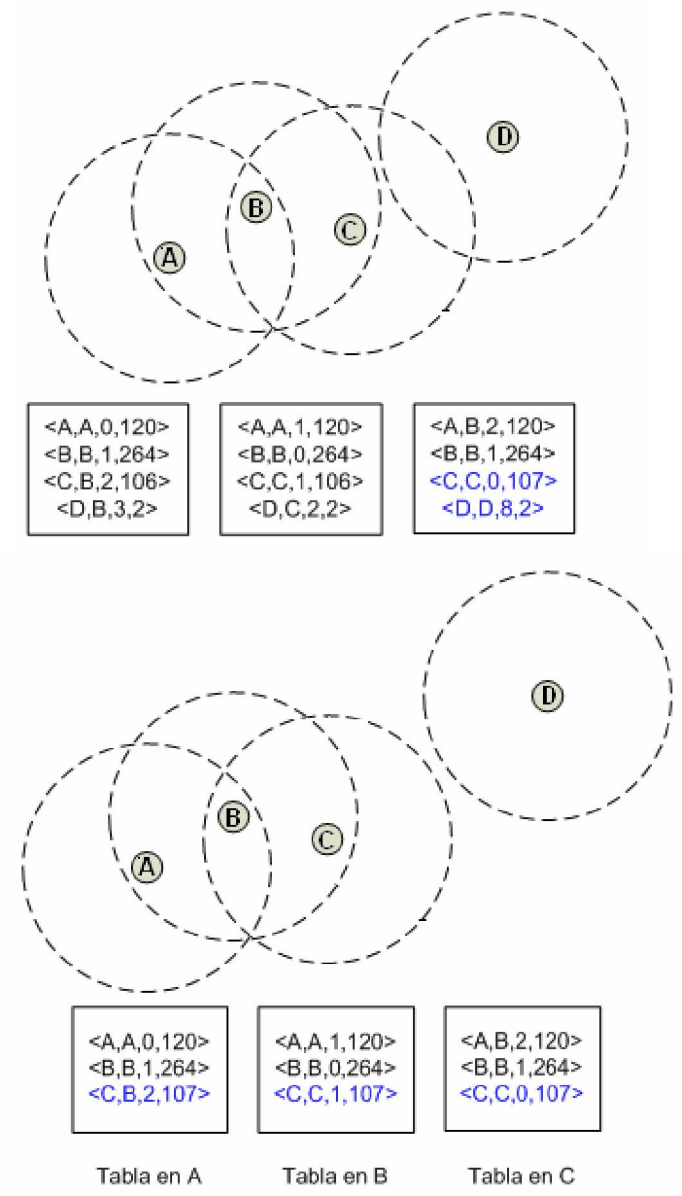


Figura. 3.12. Proceso de eliminación de una ruta con DSDV

2.11.3. Protocolo de enrutamiento AODV (*Ad-Hoc On-Demand Distance Vector Routing)*

Es un protocolo de vector distancia, es decir que su métrica está basada en el número de saltos; además se activa únicamente cuando existe la necesidad de realizar el envío de paquetes, esto significa que funciona bajo demandad. El paquete no lleva incluida la ruta que debe seguir hacia el destino, constituyéndose en un protocolo de salto a salto, en el que cado nodo es el encargado de enrutarlo hacia el siguiente, hasta alcanzar al destino.

AODV no mantiene tablas de rutas permanentes, estas tienen un tiempo de vida muy corta (*Lifetime)* y se crean básicamente mediante procesos de peticiones y respuestas de rutas hacia los otros nodos.

Descubrimiento de Rutas: Antes de enviar un paquete, el nodo origen revisa dentro de su tabla si tiene la información del siguiente salto para alcanzar el destino, si no la posee, ya sea porque es la primera vez o porque la ruta ha expirado, inicia el proceso de descubrimiento de la ruta.

En primer lugar se crea un paquete RREQ (*Route Request*) que contiene información del nodo origen, el nodo destino, un número de secuencia del origen y un contador de saltos. Este paquete es enviado mediante un broadcast hacia todos los nodos de la red, pero únicamente le enviarán una respuesta o RREP (*Route Reply)* el nodo destino o algún otro nodo que conozca una ruta hacia el nodo destino.

Cuando un nodo intermedio no conoce la ruta hacia el nodo destino, retransmite el RREQ que le llegó, pero le agrega información de cómo alcanzar al nodo origen, esto para que el nodo destino o el nodo que posee la ruta al destino puedan regresar y enviar su ruta a quien origino el RREQ. Sin embargo, el nodo intermedio no desperdicia esta información, si no posee la ruta hacia quien origino el RREQ la agregará a su tabla.

Para evitar que los RREQ inunden la red, cada nodo revisa el número de secuencia, si este coincide con uno que ya le llego anteriormente, lo descarta.

El nodo origen puede recibir varios RREP, ya que algunos nodos pueden conocer diferentes rutas para alcanzar al nodo destino, pero se analiza cual es el que tiene el menor número de saltos y se lo toma como ruta. Si por el contrario no se recibe ningún RREP, el nodo origen reenvía el RREQ pero incrementa el número de secuencia para que no sea desechado.

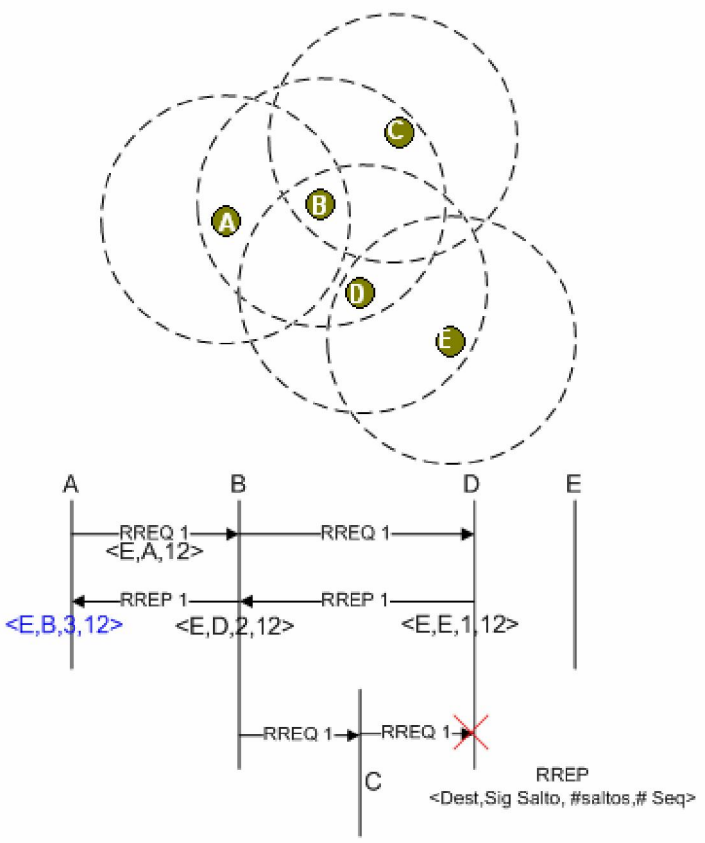


Figura. 3.13. Proceso de descubrimiento de ruta con AODV

Mantenimiento de Rutas: Las rutas se mantienen por un periodo de tiempo, después del cual son borradas de la tabla de enrutamiento, aun cuando algunas de ellas todavía sean validas y permitan alcanzar a otros nodos en la red. Sin

embargo, con esta acción se previene que existan caminos errados hacia nodos destino que pudieron haberse movido o abandonado la red o perdieron el enlace.

Cuando un nodo se mueve, será él mismo el encargado de generar las peticiones de rutas cuando necesite enviar un paquete, pero si antes de que se genere los RREP de quien cambio la topología, se envía un paquete por una ruta antigua, el primer vecino que detecta el cambio, envía un mensaje RERR (*Route Error)* a quien origino el paquete. Este mensaje RERR coloca el valor de infinito a la métrica para que los nodos descarten la ruta.

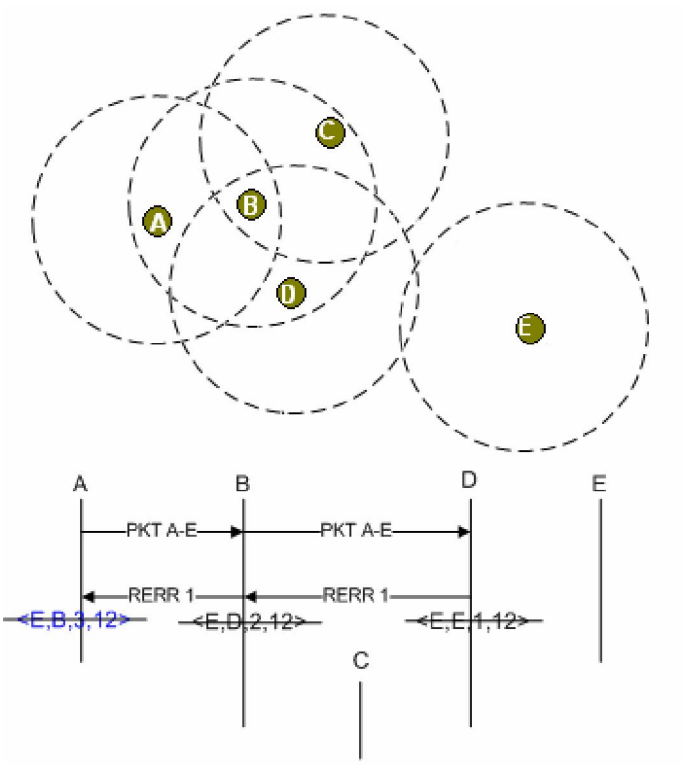


Figura. 3.14. Proceso de Eliminación de Ruta cuando pierde un enlace mediante AODV

Una de las ventajas de AODV es que puede reparar pequeñas fallas en la red, como por ejemplo si un vecino detecta que un enlace se ha caído, por su propia cuenta tratará de ubicar una nueva ruta para llegar al nodo con el que perdió el enlace, sí encuentra un camino alterno lo cambia de manera local, sin notificar a los demás nodos para evitar utilizar el ancho de banda de la red. Caso

contrario, al no encontrar una ruta, notificará a todos los nodos que usan esa ruta, para que la eliminen de su tabla.

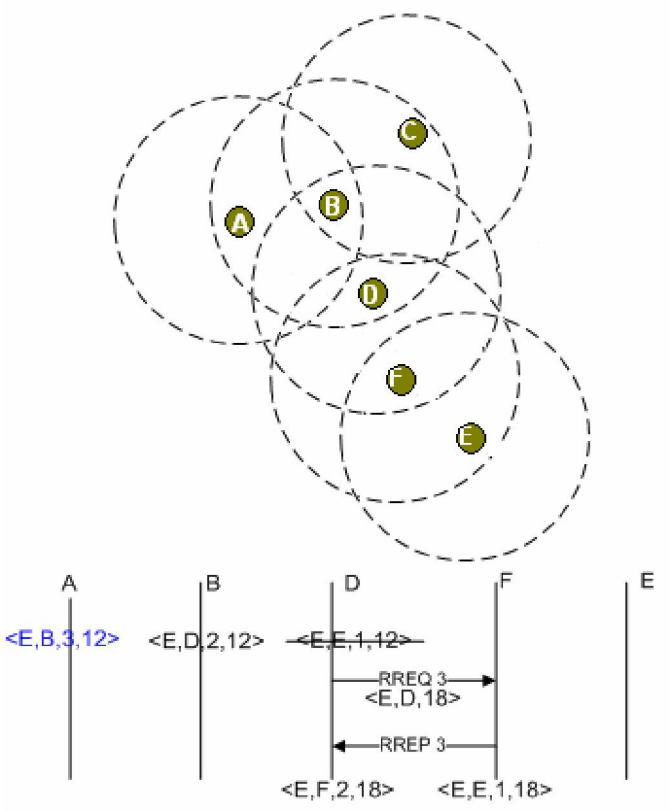


Figura. 3.15. Arreglo de una ruta perdida mediante AODV

Otra forma que posee AODV para mantener la ruta es mediante el envío de mensajes *HELLO* periódicamente, para determinar sí el enlace entre los nodos continua siendo valido.

2.11.4. Protocolo de enrutamiento DSR (*Dynamic Source Routing*)

Es un protocolo creado para redes ad-hoc con alrededor de 200 nodos móviles y con gran capacidad de movimiento. Está basado en el encaminamiento de origen, en el cual el paquete viaja con un encabezado que posee la información de los nodos debe atravesar para llegar a su destino. Además, este

protocolo trabaja bajo demanda y para optimizar completamente el ancho de banda, no realiza ningún tipo de actualización.

El protocolo trabaja con dos procesos que son el *Route Discovery* y el *Route Maintenance*

Route Discovery: Cuando un nodo necesita enviar un paquete, primero consulta en su tabla de rutas, si no consta la ruta envía un broadcast a sus nodos vecinos solicitando un *Route Request.* Este mensaje RREQ contiene la información (dirección) del nodo origen, nodo destino y un identificador de mensaje RREQ.

El mensaje RREQ atraviesa toda la red, pasando por todos los nodos. Cuando un nodo intermedio no posee la ruta para el nodo destino que se le indica, agrega su dirección al campo llamado registro de ruta y lo continua retransmitiendo.

Para evitar que las peticiones RREQ inunden la red, cada nodo analiza el identificador del mensaje, así como también, si su dirección está o no incluida en el registro de ruta, ante lo cual eliminarían la petición RREQ.

Finalmente se producirá un mensaje RREP, cuando el paquete RREQ llegue al nodo destino y utilizando la información de saltos inversos puede regresar al origen. En el caso en que no se pueda llegar al destino, o se encuentre a muchos saltos de distancia se lo considera inalcanzable y se enviará al nodo origen un mensaje de error RERR.

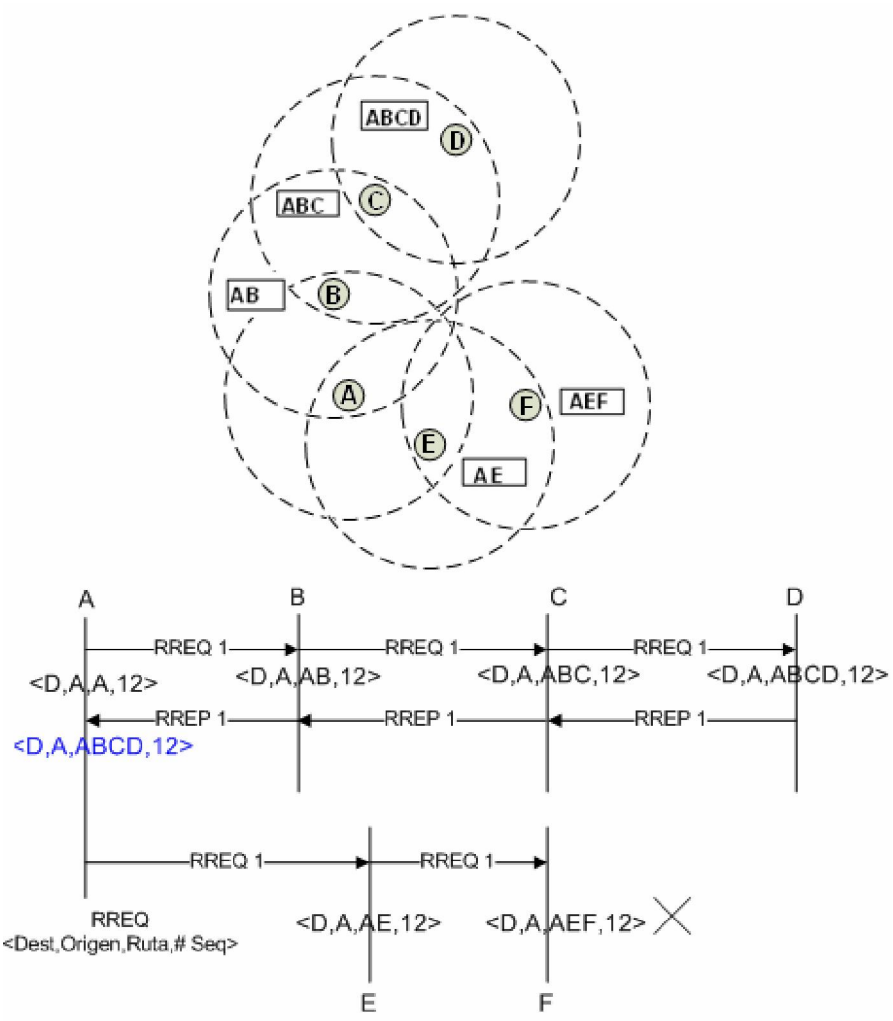


Figura. 3.16. Proceso de Descubrimiento de ruta mediante DSR

Mediante este proceso el nodo origen puede recibir varios mensajes de rutas hacia el nodo destino, pudiendo escoger las más eficientes y mantenerlas en su tabla, para cuando una falle poder usar una alterna, y de este modo no generar otra petición RREQ que utilice el ancho de banda.

Un nodo intermedio también puede responde con un RREP, si conoce la ruta hacia el nodo destino, ante lo cual enviaría el registro de ruta que le llegó y el registro de ruta que tiene para llegar al destino.

Mantenimiento de Rutas: Cuando se envía un paquete, cada nodo intermedio es responsable de comunicar si el siguiente salto hacia el destino se encuentra habilitado o no. Con este método no se recupera errores, por lo que es importante que previo al envío de un paquete, la capa MAC envíe un ACK para confirmar la validez del enlace.

Al detectar que el siguiente salto en la ruta de un nodo intermedio, no se encuentra disponible, el nodo busca un su tabla si posee una ruta alterna, si la encuentra utilizará esa nueva ruta sin notificar a los otros nodos por donde le llegó el paquete, pero al no poseer otra ruta enviará un mensaje de error RERR hacia el nodo origen para que se borre esa ruta.

2.12. PARÁMETROS PARA UNA CONFIGURACIÓN BÁSICA DE UNA RED INALÁMBRICA

Para crear los diferentes escenarios de simulación se puede tomar como base el siguiente script realizado en lenguaje Tcl, en el cual se especifica sistemáticamente, como ir creando el entorno de simulación. Los pasos que se deben seguir son los siguientes:

§ Definir las variables que serán usadas en la configuración de los nodos:

```
set val(chan)      Channel/WirelessChannel      ;#Tipo de Canal
set val(prop)      Propagation/TwoRayGround     ;#Modelo de Propagación
set val(netif)     Phy/WirelessPhy/802_15_4     ;#Tipo de interfaz de red
set val(mac)       Mac/802_15_4                 ,#Capa MAC
set val(ifq)       Queue/DropTail/PriQueue      ;#Tipo de cola
set val(ll)        LL                           ;Tipo de Capa LL
ser val(ant)       Antenna/OmniAntenna          ;Tipo de antena
set val(ifqlen)    150                          ;Max. paquete en cola
set val(nn)        25                           ;número de nodos
set val(rp)        AODV                         ;Protocolo de enrutamiento
set val(x)         60                           ;dimensión x de topología
set val(y)         60                           ;dimensión y de topología
```

§ Creación del Planificador o Despachador de Tareas, que es una instancia de la clase Simulator, que permitirá después armar y configurar la simulación

```
set ns [new Smulator]          ;#set (comando de asignación)
                               ;# ns objeto de la clase Simulator
```

§ Creación del archivo de traza y de visualización gráfica

```
#Creación de archivo de traza
set tracefile [open ejemplo.tr w]
$ns trace-all $tracefile

#Creación de archivo NAM
set namtrace     [open ejemplo.nam w]
$ns namtrace-all-wireless $namtrace $val(x) $val(y)
```

§ Establecer los parámetros de la topología

```
set topo [new Topography]
$topo load_flatgrid $val(x) $val(y)
```

§ Definir el archivo que simulará todos los eventos (GOD - *General Operations Director)*

```
set god_ [create-god $val(nn)]
set chan_1_ [new $val(chan)]
$ns use-newtrace
```

§ Establecer la configuración de los nodos en base a las variables anteriormente creadas

```
$ns node-config -propType
$ns node-config -adhocRouting $val(rp) \
                -llType $val(ll) \
                -macType $val(mac) \
```

```
        -ifqType $val(ifq) \
        -ifqLen $val(ifqlen) \
        -antType $val(ant) \
        -propType $val(prop) \
        -phyType $val(netif) \
        -topoInstance $topo \
        -agentTrace ON \
        -routerTrace ON \
        -macTrace ON \
        -movementTrace OFF \
        -channel $chan_1_
```

- Crear los nodos

```
for {set i 0} {$i < $val(nn) } {incr i} {
        set node($i) [$ns node]
        $node($i) random-motion 0              ;# disabilitar  random motion
    }
```

- Establecer la posición de los nodos, mediante coordenadas

```
$node(0) set X_ 42.4
$node(0) set Y_ 9.9
$node(0) set Z_ 0.0
```

- Para los nodos móviles se utiliza el siguiente comando:

```
$ns at 0.5 "$node(8) setdest 52 30 5"    ;#at-> indica el tiempo, setdest-> posición
                                         ;#x y; 5 es la velocidad de movimiento
```

- Determinar el tamaño de los nodos en el simulador

```
for {set i 0} {$i < $val(nn)} {incr i} {
        $ns initial_node_pos $node($i) 3
    }
```

- Establecer las conexiones entre los nodos y en base al tipo de trafico que se requiere enviar

```
#TCP origen
set tcp0 [new Agent/TCP]
$ns attach-agent $node(18) $tcp0
#eval \$tcp0 set packetSize_ 20
#TCP Desdino
set sink0 [new Agent/TCPSink]
$ns attach-agent $node(6) $sink0
#Enlace
$ns connect $tcp0 $sink0
$tcp0 set fid_ 0
set ftp0 [new Application/FTP]
$ftp0 attach-agent $tcp0
    $ns at 0.0 "$ftp0 start"
```

- Proceso de finalización

```
$ns at 150 "$ftp0 stop"
$ns at 150 "$ns nam-end-wireless 150"
$ns at 150 "finish"

proc finish {} {
   global ns namtrace tracefile
   $ns flush-trace
   close $namtrace
   close $tracefile
   exec nam a-25-2r.nam &
   exit 0
    }
```

- Correr el simulador

```
$ns run
```

CAPÍTULO 4

ANÁLISIS DEL DESEMPEÑO DE LOS ESCENARIOS DE RED SIMULADOS

Para desarrollar las simulaciones que se analizan en este capitulo y que son el objetivo principal del desarrollo de esta tesis, se utilizó el programa *Network Simulator* versión 2.32. El cual consta con las librerías necesarias para implementar una *Wireless Personal Area Network* (WPAN) y específicamente una red Ad-Hoc con nodos móviles (MANET – *Movil Ad-Hoc Network*), con la posibilidad de variar los modelos de propagación entre *Free Space, Shadowing* o *Two-Ray Ground.*

El protocolo de enrutamiento que se utilizó es AODV (*Ad-Hoc On-Demand Distance Vector),* ya que el protocolo DSDV (*Destination Sequenced Distance Vector)* y el protocolo DSR (*Dynamic Source Routing*), utilizan paquetes de enrutamiento que superan los 127 bytes que establece el estándar IEEE 802.15.4 para realizar el envío de una trama.

Para poder obtener los datos necesarios para realizar el análisis, se utilizó el programa TraceGraph 2.02, el cual permite visualizar de manera gráfica los datos resultantes de la simulación de los archivos de traza (*.tr). Este programa creado por *Jaroslaw Malek*, esta desarrollado sobre la plataforma de programación que ofrece Matlab y sus respectivas librerías. Se lo puede descargar de la dirección web *http://www.tracegraph.com./*

Otro programa de gran utilizad es Trace Converter v1.01, que permite adecuar el archivo de traza resultante del simulador NS-2, a un formato que es mas fácil de interpretar por parte de Trace Graph, disminuyendo el tiempo que toma cargar el archivo .tr común, en el analizador gráfico Trace Graph.

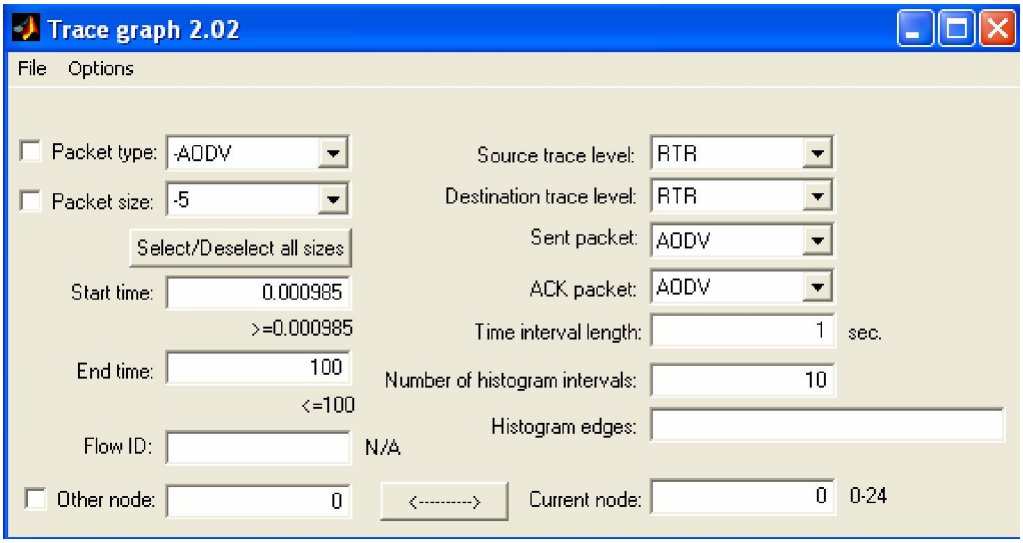
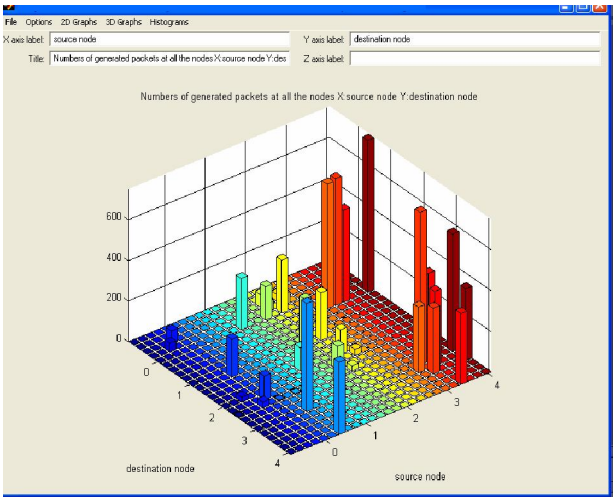
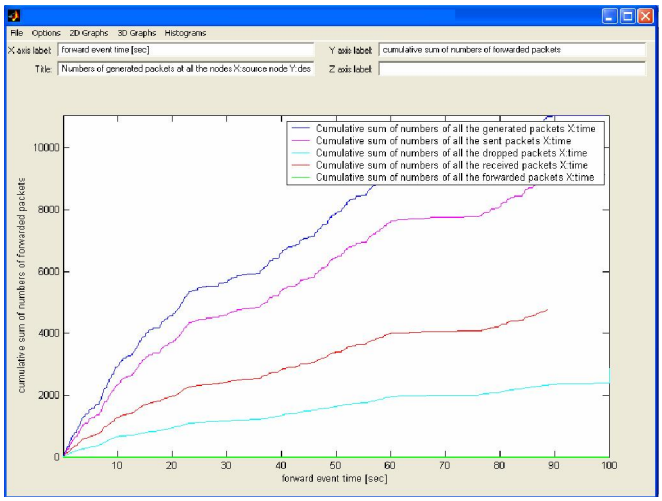


Figura. 4.1. Ventana de TraceGraph para Cargar el Archivo de Traza

En la Figura. 4.1 se muestra la primera ventana que se ejecuta al abrir TraceGraph. Una vez que se a cargado el archivo de traza, con el formato resultante del programa Trace Converter, se puede escoger entre varias opciones que información será mostrada en las otras ventanas que posee el programa. Se puede seleccionar que tipo de paquetes se visualizará, como por ejemplo paquetes de enrutamiento o paquetes TCP. En esta ventana también se puede especificar entre que nodos se mostrará la información.

En la Figura. 4.2 a),b) y c) se muestran las tres posibles formas de ver los datos de la simulación, ya sean en gráficos 3D, 2D o mediante el uso de histogramas





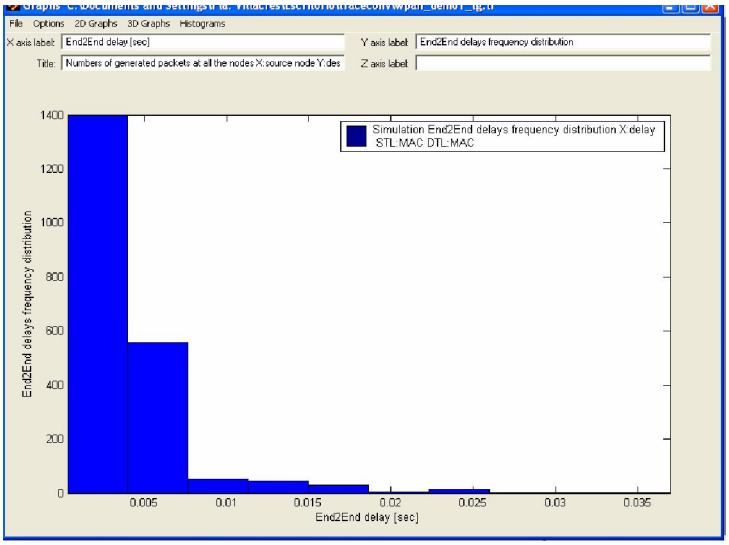


Figura. 4.2. a) Visualización en 3D; b) Visualización de 2D; c) Visualización mediante histogramas

La tercera ventana que posee el programa Trace Graph, que se puede observar en la Figura 4.3. es la encargada de mostrar los datos de manera estadística, presenta datos de manera general de toda la red, así como también de un solo nodo que se haya seleccionado anteriormente.

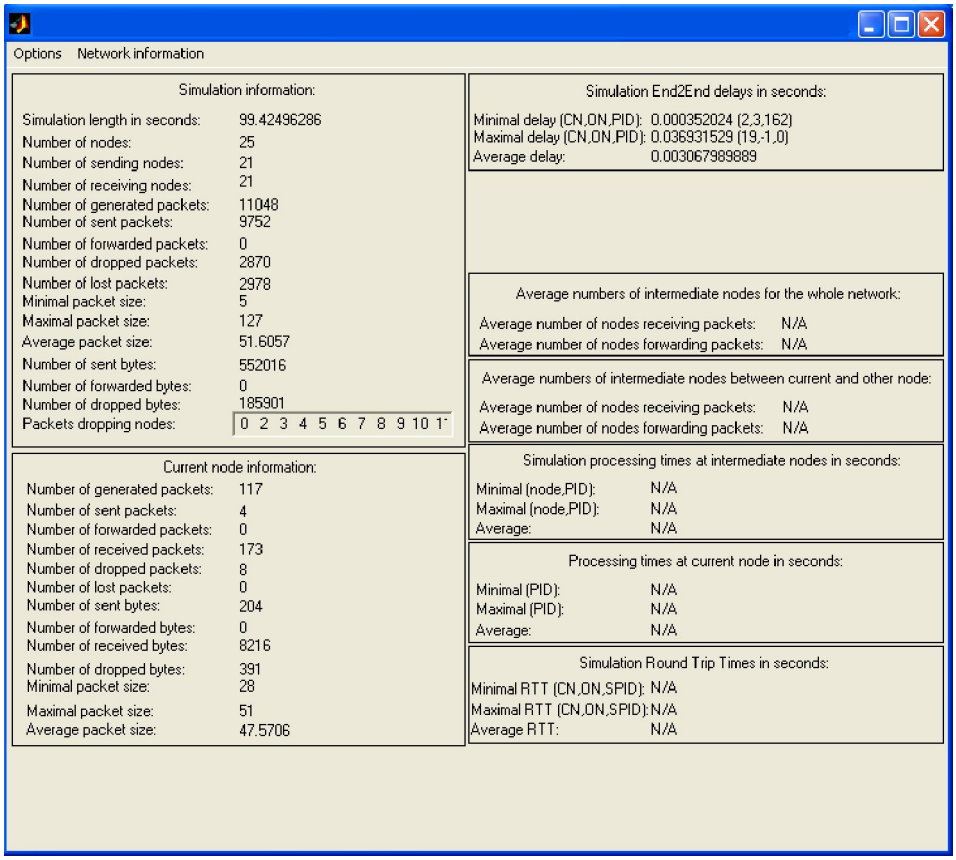


Figura. 4.3. Ventana de datos estadísticos de Trace Graph

2.13. PARÁMETROS PARA EL ANÁLISIS

Para realizar el análisis de una red inalámbrica se tiene ciertas métricas o parámetros que se pueden considerar para determinar su comportamiento o confiabilidad, como los que se mencionan a continuación:

2.13.1. Throughput de la Red

Es uno de los parámetros más importantes en el análisis del funcionamiento de una red, que indica la cantidad de datos transmitidos en bytes, en un determinado periodo de tiempo expresado en segundos. Este indicador nos permite conocer el nivel de rendimiento de la red, es decir la capacidad que tiene la red para manejar la información que circula en ella.

El throughput puede ser calculado en un nodo o para toda la red. La fórmula para calcular este parámetro es la siguiente:

$$Throughput\ de\ \mathrm{Re}d = \frac{Bytes\ totales\ Transmitidos}{Tiempo\ de\ Transmisión\ (seg)}$$

2.13.2. Retardo de Extremo a Extremo (*End to End Delay*)

Representa el tiempo que transcurre desde que un paquete sale del nodo origen hasta que alcanza el nodo destino. Los paquetes que son considerados dentro de este parámetro son únicamente los que fueron transmitidos y recibidos exitosamente. La forma para calcular el tiempo promedio del retardo extremo a extremo es la siguiente:

$$Promedio\ de\ Retardo = \frac{Suma\ de\ retardos\ de\ todos\ los\ paquetes}{Total\ de\ paquetes\ recibidos}$$

Mediante el programa Trace Graph se puede obtener directamente el valor del retardo promedio de la red, así como también del retardo máximo y mínimo que se obtuvo en el envío y recepción de un paquete.

2.13.3. Relación de Entrega (*Delivery Ratio)*

Indica el porcentaje de los paquetes que fueron recibidos con éxito y nos permite tener una visión del congestionamiento presente en la red, constituyéndose en un indicador muy importante al momento de analizar el desempeño de los paquetes. La forma de calcular este parámetro esta dada por la siguiente fórmula:

$$Delivery\ Ratio = \frac{Número\ de\ Paquetes\ recibidos}{Número\ de\ Paquetes\ Transmitidos} \times 100$$

2.14. **ESCENARIOS PARA LAS SIMULACIONES**

Para poder realizar el análisis de una red WPAN basada en el estándar IEEE 802.15.4, se crearon cinco escenarios, conformados por 10, 17, 25, 40 y 50 nodos respectivamente.

Cada escenario estará ubicado en un área de 60x60 m^2 y se irá variando su modelo de propagación entre Dos Rayos, Shadowing y Free Space. Los nodos dispuestos en cada escenario estarán configurados para formar una MANET (Movil Ad-Hoc Network), es decir existirán únicamente nodos fijos.

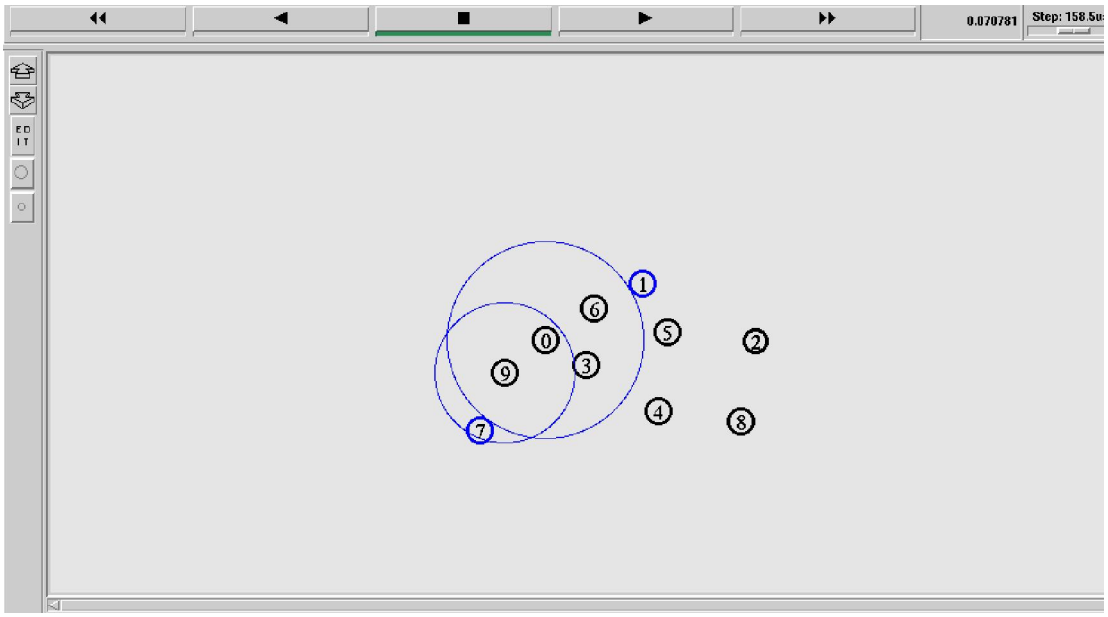


Figura. 4.4. Escenario de 10 nodos (Transmisión del nodo 7 hacia el nodo 1)

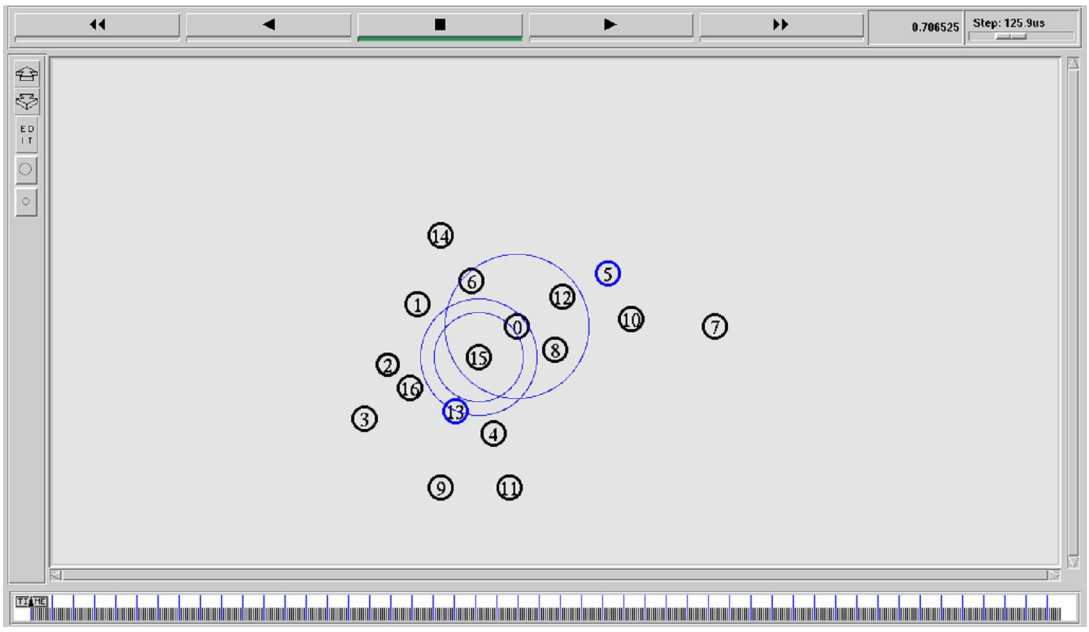


Figura. 4.5. Escenario de 17 nodos (Transmisión del nodo 13 hacia el nodo 5)

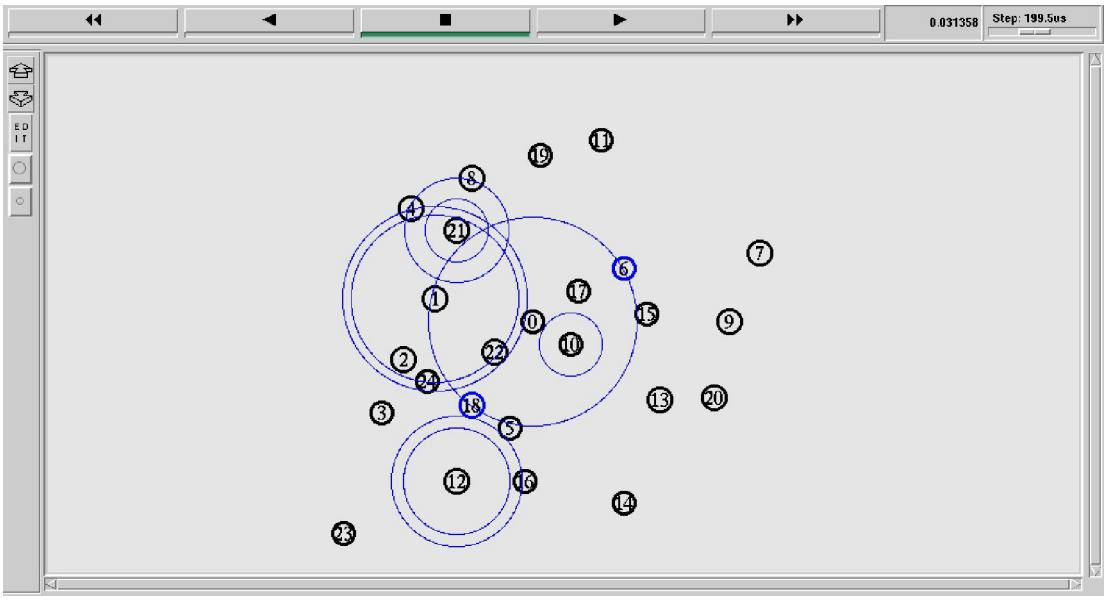


Figura. 4.6. Escenario de 25 nodos (Transmisión del nodo 18 hacia el nodo 6)

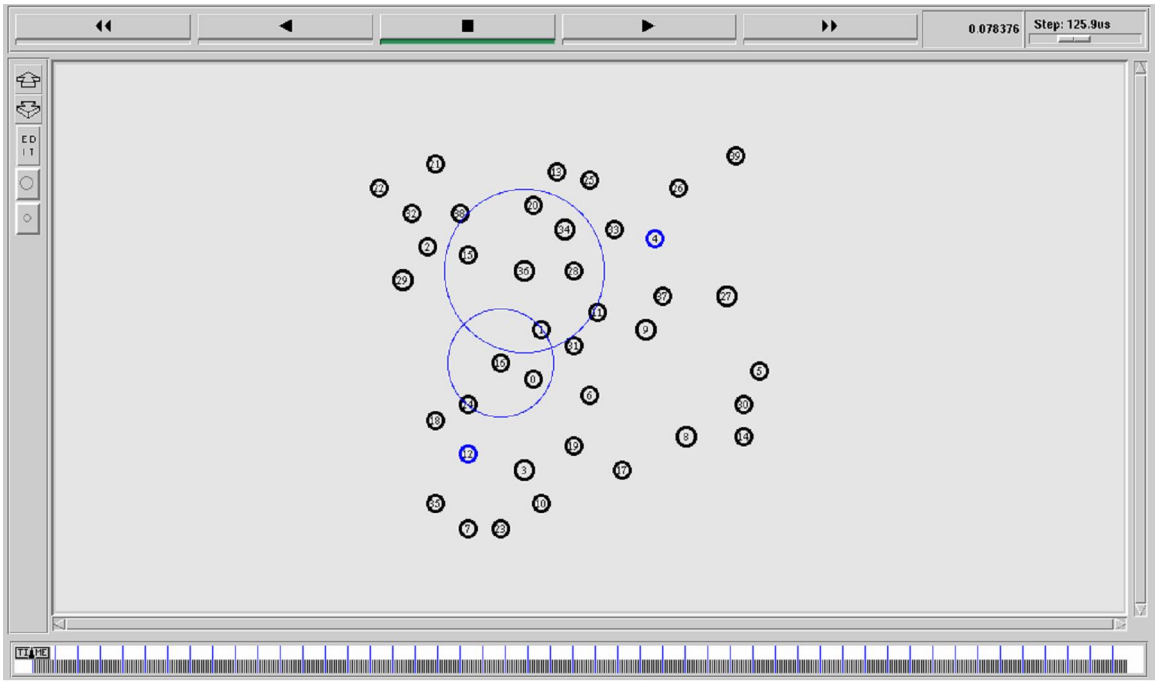


Figura. 4.7. Escenario de 40 nodos (Transmisión del nodo 12 hacia el nodo 4)

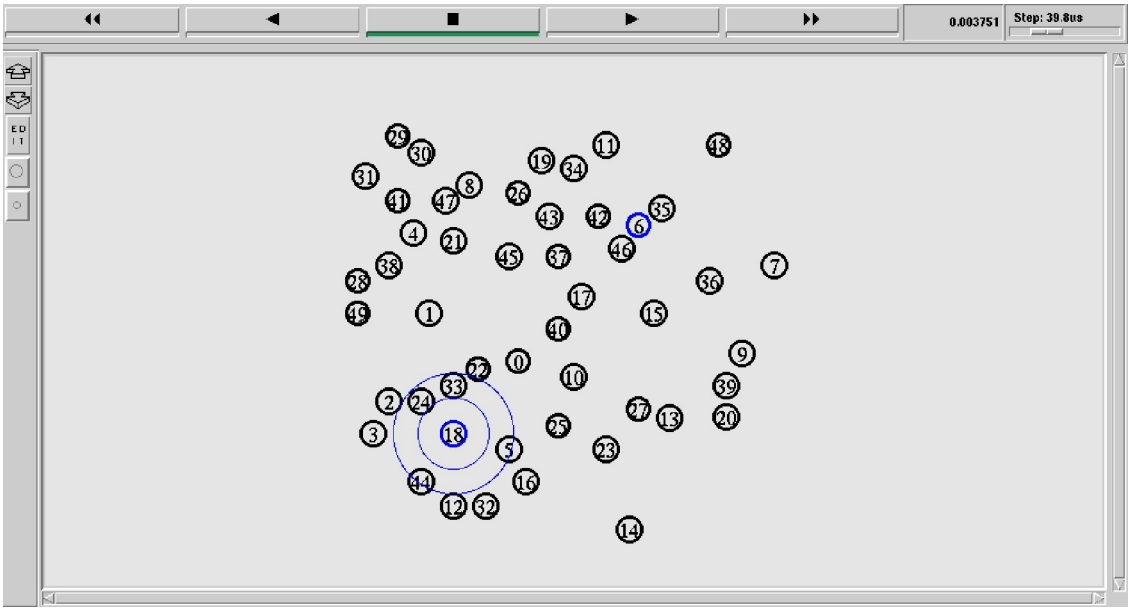


Figura. 4.8. Escenario de 50 Nodos (Transmisión del nodo 18 hacia el nodo 6)

A continuación se detallan las características de cada escenario que se creará mediante el programa NS-2.32:

Tabla 4.1. Características Generales de los Escenarios

ESCENARIOS	
Nº de Nodos Fijos	10, 17, 25, 40, 50
Nº de Nodos Móviles	0
Modelo de Propagación	Dos Rayos / Free Space / Shadowing
Protocolo de Enrutamiento	AODV
Área	60x60 m2
Capa Física	802.15.4 (914 MHz)
Radio de Cobertura de los nodos	~10 a 15 (m)

Tabla 4.2. Escenarios para el modelo de Propagación Shadowing

Escenario	10 Nodos	17 Nodos	25 Nodos	40 Nodos	50 Nodos
Nodo Transmisor	7	13	18	12	18
Nodo Receptor	1	5	6	4	6
Tipo de Tráfico	TCP / FTP	TCP / FTP	TCP / FTP	TCP / FTP	TCP / FTP

2.15. ANÁLISIS DE LOS DIFERENTES ESCENARIOS DE SIMULACIÓN

A partir de las simulaciones y con la ayuda del programa TraceGraph 2, que permite visualizar los datos contenidos en los archivos de traza, se obtuvieron los siguientes resultados que se muestran en los cuadros, para cada modelo de propagación con la respectiva densidad de nodos.

Tabla 4.3. Resultados para el modelo de Propagación de Dos Rayos

Modelo de Propagación de Dos Rayos					
Densidad de Nodos	10	17	25	40	50
Paquetes Generados	2858	2678	2409	3252	2384
Paquetes Enviados	2668	2428	1974	2205	1686
Paquetes Recibidos	399	287	226	191	105
Paquetes Caídos	465	528	427	2035	4098
Paquetes AODV	898	1175	1261	2242	1958
Bytes Generados	199810	179830	157310	200820	140290
Bytes Enviados	187140	164460	132360	142770	101250
Bytes Recibidos	26876	19284	15184	12736	7004
Bytes Recibidos TCP	15260	11260	8860	7340	3580
Bytes Caídos	32826	35648	28205	116010	227050
Retardo Mínimo (seg)	0,01908	0,01652	0,01716	0,01588	0,01583
Retardo Máximo (seg)	0,10334	0,099041	0,35616	1,2979	2,34558
Retardo Promedio (seg)	0,04245	0,038413	0,03914	0,063581	0,1141
Duración de la simulación (seg)	583,536	549,52	553,08	579,03	555,048
Duración de la transmisión (seg)	55,2592	122,6355	148,25	89,7285	85,612

Tabla 4.4. Resultados para el modelo de Propagación Free Space

Modelo de Propagación Free Space					
Densidad de Nodos	10	17	25	40	50
Paquetes Generados	6457	12472	4870	6313	4653
Paquetes Enviados	5913	9968	4429	4332	3132
Paquetes Recibidos	853	1536	606	612	326
Paquetes Caídos	1414	3533	941	2736	1337
Paquetes AODV	2046	4621	1755	3596	2785
Bytes Generados	451100	856700	405360	451550	316980
Bytes Enviados	416600	712970	373070	341030	232860
Bytes Recibidos	57236	102890	52336	41164	22352
Bytes Recibidos TCP	103500	59740	35340	20080	11960
Bytes Caídos	97723	222490	80473	169160	83784
Retardo Mínimo (seg)	0,01588	0,01652	0,01652	0,01716	0,02750
Retardo Máximo (seg)	0,39901	4,21620	4,44643	5,16988	9,17550
Retardo Promedio (seg)	0,038859	0,039654	0,045360	0,117696	0,167410
Duración de la simulación (seg)	594,02	589,519	560,7898	593,16	571,04
Duración de la transmisión (seg)	507,1421	319,0215	560,762	582,83	563,629

Tabla 4.5. Resultados para el modelo de Propagación Shadowing

Modelo de Propagación Shadowing					
Densidad de Nodos	10	17	25	40	50
Paquetes Generados	2034	2141	2653	1775	1734
Paquetes Enviados	1233	1384	1041	756	500
Paquetes Recibidos	254	196	155	108	72
Paquetes Caídos	872	1540	3926	6190	10500
Paquetes AODV	1029	1310	1733	1398	1460
Bytes Generados	145980	143930	187690	111860	104600
Bytes Enviados	95283	96284	95323	53754	34512
Bytes Recibidos	19184	13808	25940	8168	5384
Bytes Recibidos TCP	11560	7720	17100	4900	3360
Bytes Caídos	54832	88345	219140	339340	578940
Retardo Mínimo (seg)	0,01215	0,01130	0,01450	0,01034	0,01537
Retardo Máximo (seg)	1,14495	1,49793	1,51012	2,08890	1,49310
Retardo Promedio (seg)	0,06784	0,08680	0,07948	0,20450	0,22056
Duración de la simulación (seg)	600	570,52	577,52	566,02	301,53
Duración de la transmisión (seg)	76,38	151,52	409,072	557,5	292,744

2.15.1. Análisis de Throughput de la Red

A continuación se realizará el análisis y la comparación entre los diferentes modelos de propagación que se pueden configurar en NS-2.

Para conocer la cantidad de bytes transmitidos se tomó como referencia los bytes efectivamente recibidos; por lo que, de los datos obtenidos en el analizado de trazas TraceGraph, se usó los bytes TCP recibidos para realizar el cálculo del Throughput de Red.

Adicionalmente se calculó el Throughput Normalizado que resulta de dividir el Throughput de Red para la tasa de transmisión, que para las simulaciones era de 20 Kbps.

Los datos que se obtuvieron son los que se encuentran expresados en la siguiente tabla:

Tabla 4.6. Valores del Throughput de Red

Modelo de Propagación Dos Rayos					
Densidad de Nodos	10	17	25	40	50
Bytes Recibidos TCP	15260	11260	8860	7340	3580
Duración de la trasmisión (seg)	55,2592	122,6355	148,25	89,7285	85,612
Throughput de Red(Kbps)	2,157	0,717	0,467	0,639	0,327
Throughput normalizado	0,108	0,036	0,023	0,032	0,016
Modelo de Propagación Free Space					
Densidad de Nodos	10	17	25	40	50
Bytes Recibidos TCP	103500	59740	35340	20080	11960
Duración de la trasmisión (seg)	507,1421	319,0215	560,762	582,83	563,629
Throughput de Red(kbps)	1,594	1,463	0,492	0,269	0,166
Throughput normalizado	0,080	0,073	0,025	0,013	0,008
Modelo de Propagación Shadowing					
Densidad de Nodos	10	17	25	40	50
Bytes Recibidos TCP	11560	7720	17100	4900	3360
Duración de la trasmisión (seg)	76,38	151,52	409,072	557,5	292,744
Throughput de Red(kbps)	1,182	0,398	0,327	0,069	0,090
Throughput normalizado	0,059	0,020	0,016	0,003	0,004

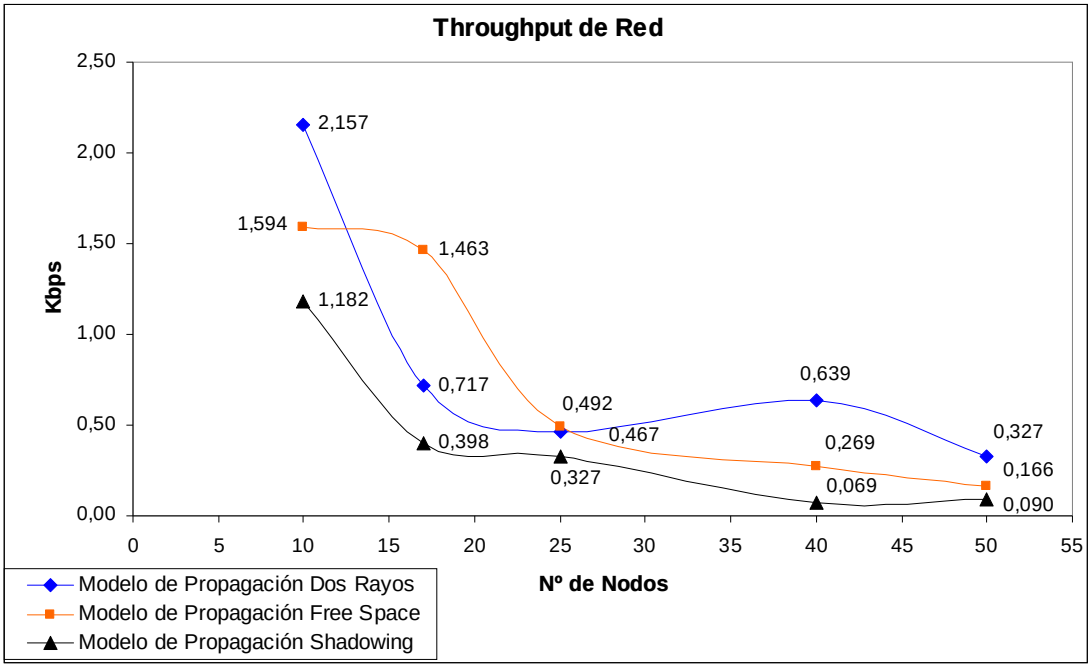


Figura. 4.9. Throughput de Red

El Throughput de la Red decrementa su valor al aumentar la densidad de nodos en el área de simulación; esto debido a que existen más dispositivos que generen tráfico y a su vez también producen mayor cantidades de colisiones. Esto significa que el nodo origen va a tener que reenviar los paquetes que no se transmitieron, provocando que la misma cantidad de bytes lleguen efectivamente en un mayor periodo de tiempo que en los escenarios con menor número de nodos, reflejándose en la disminución del Throughput de red.

Se puede observar en la Figura. 4.9. que el decremento del Throughput en función de la densidad de nodos no es lineal, debido a que las conexiones que se establecen entre los nodos tampoco siguen un comportamiento lineal.

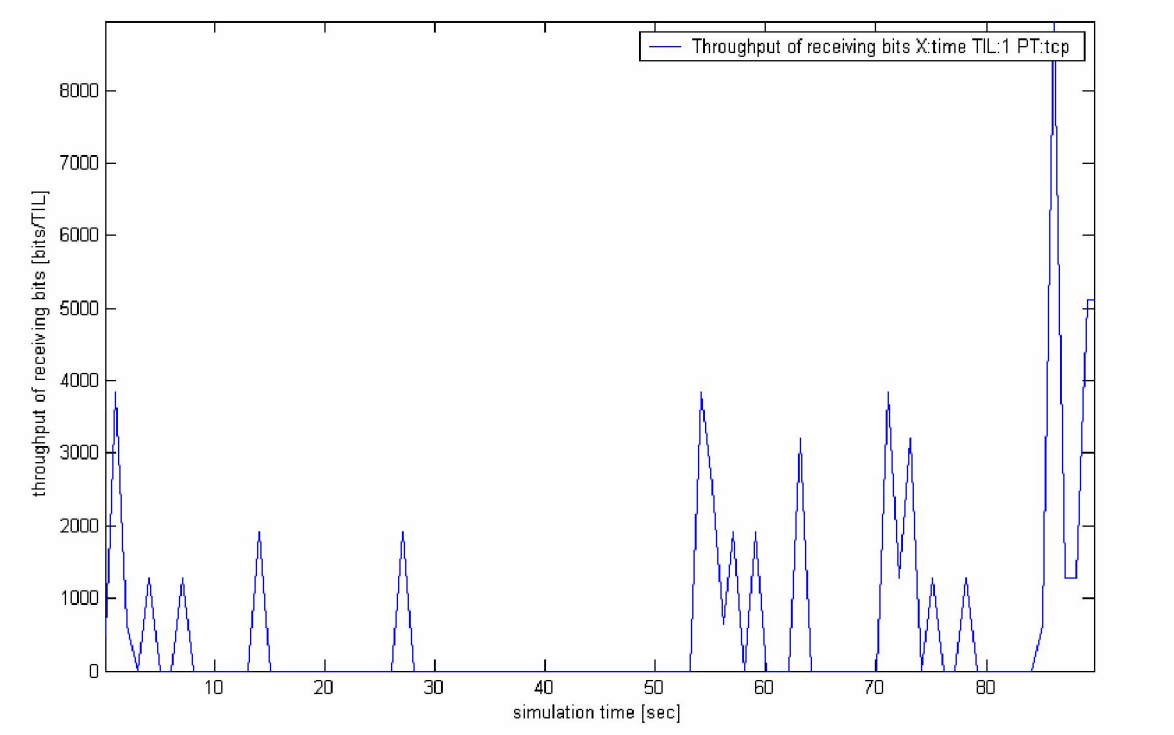


Figura. 4.10. Throuhput de Red para el escenario de Dos Rayos con 25 Nodos

El Throughput que se calcula con la fórmula se podría decir que es un promedio, ya que como se ve en la Figura. 4.10. el Througpuht de red alcanza valores superiores a los 8 Kbps, pero también existen periodos de tiempo en los que no se envía ningún bit, esto afecta a los resultados obtenidos con la fórmula, mediante la cual parece que la tasa de transmisión llega a caer mas del 90%; pero sin embargo, refleja la realidad de que el rendimiento de la red decrece.

Desde el punto de vista de los modelos de propagación, asumir un comportamiento como el de Dos Rayos, siguiere que la red obtendrá mejores resultados tanto para pocos nodos, como para una gran densidad de ellos; ya este modelo únicamente se ve afectado por reflexiones en la tierra cuando las distancias son grandes, lo cual no ocurre en estos escenarios de pruebas. Para el modelo de Shadowing, se puede apreciar que los desvanecimientos de la señal que se asumen en el simulador, le afectan de gran manera en su Throughput de red, siendo el modelo que en los cinco escenarios tiene el menor rendimiento.

2.15.2. Análisis del Delay End-to-End

Los datos correspondientes a este parámetro se los obtuvo directamente del programa analizador de trazas TraceGraph, por lo que no fue necesario realizar ningún cálculo extra, ni aplicar la respectiva fórmula para obtener su valor.

En la siguiente tabla se muestran los resultados obtenidos relacionados a los retardos máximos, mínimos y promedios, para cada escenario:

Tabla 4.7. Datos del Delay End-to-End el los diferentes modelos de propagación

Modelo de Propagación Dos Rayos					
Densidad de Nodos	10	17	25	40	50
Retardo Mínimo (seg)	0,01908	0,01652	0,01716	0,01588	0,01583
Retardo Máximo (seg)	0,10334	0,099041	0,35616	1,2979	2,34558
Retardo Promedio (seg)	0,04245	0,038413	0,03914	0,063581	0,1141
Modelo de Propagación Free Space					
Densidad de Nodos	10	17	25	40	50
Retardo Mínimo (seg)	0,01588	0,01652	0,01652	0,01716	0,02750
Retardo Máximo (seg)	0,39901	4,21620	4,44643	5,16988	9,17550
Retardo Promedio (seg)	0,038859	0,039654	0,045360	0,117696	0,167410
Modelo de Propagación Shadowing					
Densidad de Nodos	10	17	25	40	50
Retardo Mínimo (seg)	0,01215	0,01130	0,01450	0,01034	0,01537
Retardo Máximo (seg)	1,14495	1,49793	1,51012	2,08890	1,49310
Retardo Promedio (seg)	0,06784	0,08680	0,07948	0,20450	0,22056

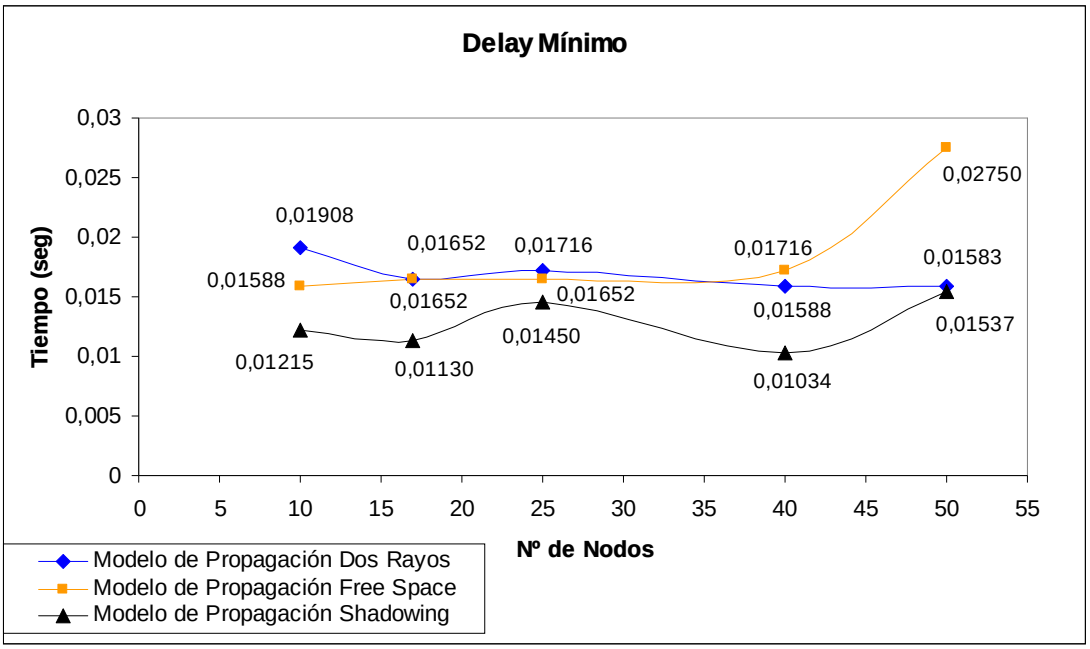


Figura. 4.12. Retardo Mínimo en el envío de un paquete

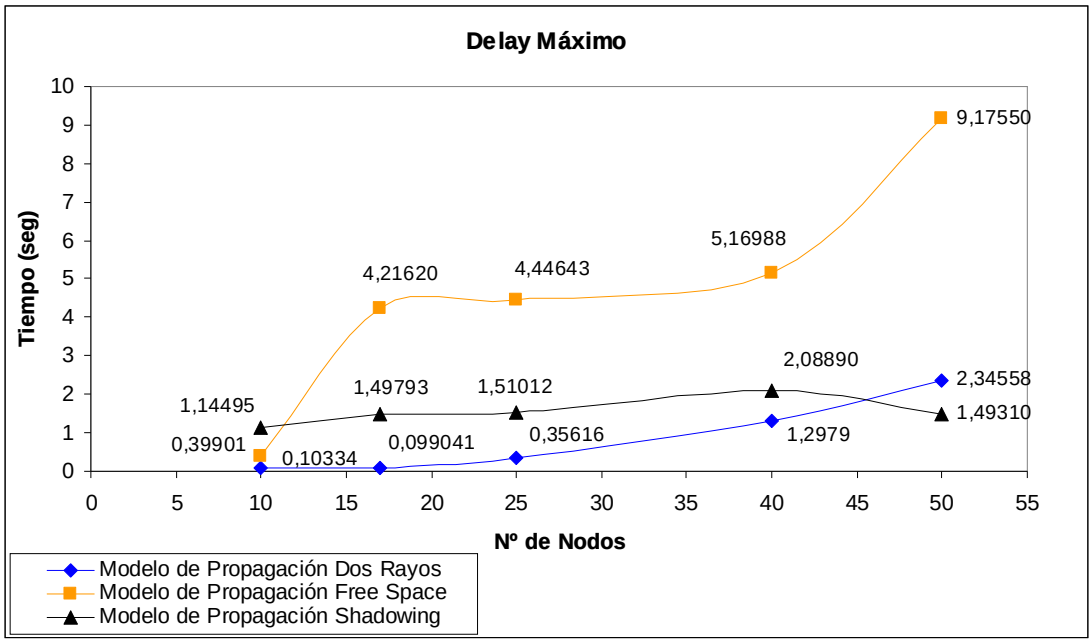


Figura. 4.13. Retardo Máximo en el envío de un paquete

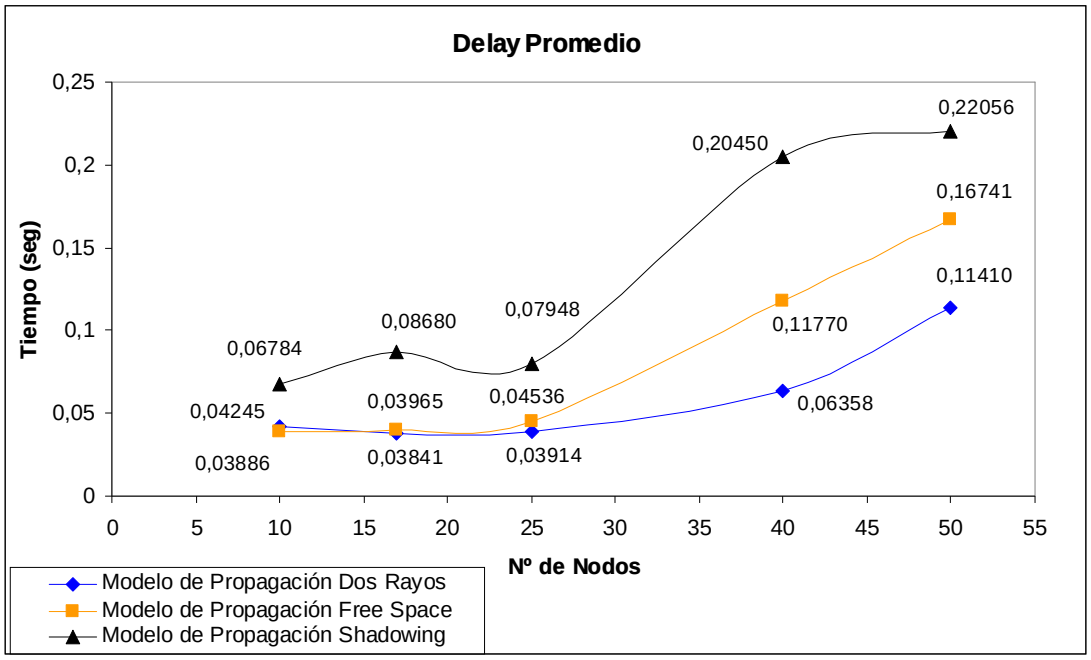


Figura. 4.14. Retardo Promedio en el envío de paquetes

Como se puede observar en las figuras 4.12, 4.13 y 4.14 el retardo o tiempo que le toma llegar a un paquete desde el origen hacia el destino, tiene una tendencia a aumentar conforme aumenta también la densidad de nodos presentes en la red. Esto debido obviamente, a que el paquete tiene que transitar y ser enrutado por un mayor número de dispositivos.

Analizando la Figura 4.12 se puede señalar que el modelo de Dos Rayos no se ve seriamente afectado por el aumento en la cantidad de nodos que conformar la red, ya que su retardo mínimo varía escasamente en los cinco diferentes escenarios. Para los otros dos modelos de propagación el tiempo mínimo de entrega de un paquete posee una tendencia a aumentar conforme se incrementa la densidad de nodos

Para el caso del parámetro que nos indica el mayor tiempo que le toma a un paquete llegar al destino, se observa en la Figura 4.13 que el tiempo transcurrido en segundos, se incrementa considerablemente a medida que aumenta la densidad de nodos. En esta figura, el modelo de propagación Free Space es el que tiene los tiempos de entrega mas elevados, ya que como no considera desvanecimientos, obstáculos o reflexiones en la Tierra, posee mayor cantidad de posibles rutas, pero que por la cantidad de saltos pueden resultar ineficientes, provocando que un paquete se tarde algunos segundos en llegar a su destino.

La Figura 4.14 corresponde al retardo promedio de entrega de un paquete durante todo el tiempo que duró la simulación. La tendencia para los tres modelos de propagación es la misma, es decir el tiempo de entrega de un paquete aumenta conforme también aumenta la densidad de nodos presentes en la red. En general, el modelo de propagación Shadowing es el que mas se tarda en entregar un paquete en el nodo destino, mientras que los modelos de propagación Free Space y Dos Rayos tienen un comportamiento muy similar para escenarios con pocos nodos, al incrementarse el número de nodos Free Space se tarda mas en entregar un paquete.

2.15.3. **Análisis de *Delivery Ratio* de la Red**

Los datos obtenidos para poder calcular este parámetro son los que se encuentran en la siguiente tabla y la fórmula que se utilizó es la que se explicó en la sección 4.1.3. de este capítulo:

Tabla 4. 8 Datos para Calcular el parámetro Delivery Ratio

Modelo de Propagación Dos Rayos					
Densidad de Nodos	10	17	25	40	50
Paquetes Enviados	2668	2428	1974	2205	1686
Paquetes Recibidos	399	287	226	191	105
Delivery Ratio (%)	14,96	11,82	11,45	8,66	6,23
Modelo de Propagación Free Space					
Densidad de Nodos	10	17	25	40	50
Paquetes Enviados	5913	9968	4429	4332	3132
Paquetes Recibidos	853	1536	606	612	326
Delivery Ratio (%)	14,43	15,41	13,68	14,13	10,41
Modelo de Propagación Shadowing					
Densidad de Nodos	10	17	25	40	50
Paquetes Enviados	1233	1384	1041	756	500
Paquetes Recibidos	254	196	155	108	72
Delivery Ratio (%)	20,60	14,16	14,84	14,29	14,40

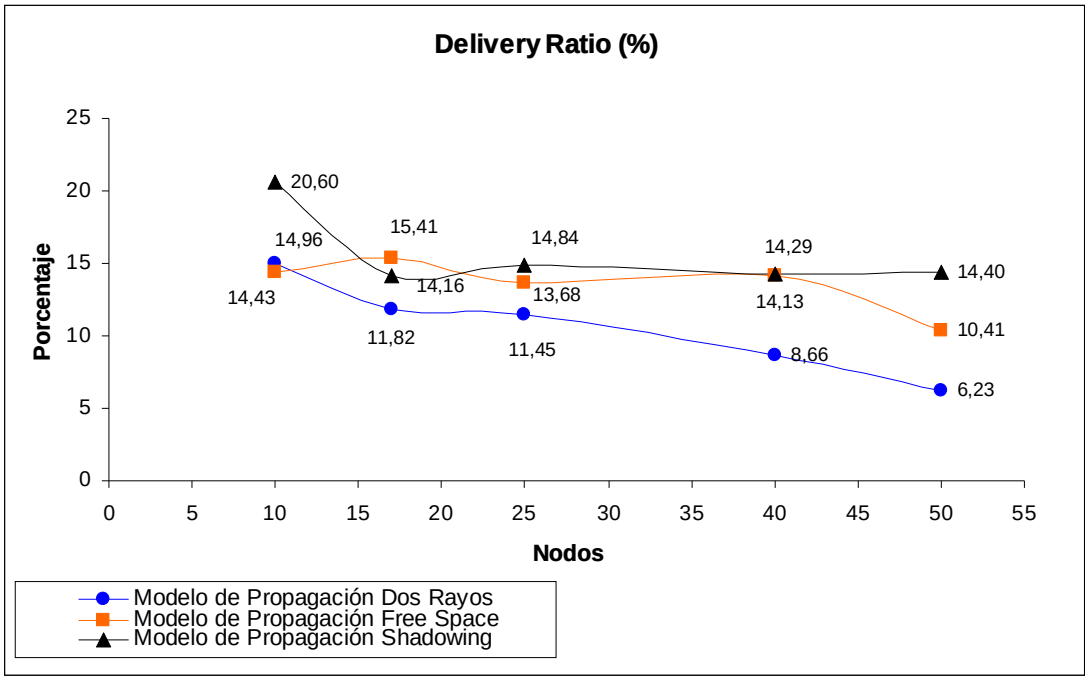


Figura. 4.15 Delivery Ratio de los tres modelos de propagación

Mediante la figura 4.15 que se generó en base a los datos obtenidos en las simulaciones, se puede determinara que la tasa de entrega de paquetes (*Delivery Ratio)*, tiende una tendencia a disminuir conforme aumenta la cantidad de nodos que conforman la red.

Esta disminución en la capacidad de la red para entregar los paquetes que se generan, se debe principalmente a que aumenta el número de colisiones al aumentar la densidad de nodos. Como consecuencia de las colisiones, los paquetes enviados no logran alcanzar a su destino, por lo que tienen que ser reenviados, esto genera que el total de paquetes que un nodo envía efectivamente en el período de simulación sea mucho mayor a los paquetes que se logra que el nodo destino reciba. Este proceso disminuye el porcentaje de paquetes entregados (*Delivery Ratio)*.

De igual forma en la Figura 4.15 también se observa que la tasa de entrega de paquetes no logra valores muy altos, es decir que para este tipo de WPAN el *Delivery Ratio* no es un parámetro favorable, se lo puede considerar como un limitante frente a otros estándares usados para comunicar redes de área personal.

De los tres modelos de propagación, el que alcanza el menor porcentaje de entrega de paquetes es Dos Rayos, mientras que el modelo de Shadowing alcanza los valores más altos en casi todos los escenarios simulados mediante el programa NS-2.32.

Para escenarios con alta densidad de nodos, el modelo de propagación Dos Rayos mantiene una tendencia fija en el porcentaje de entrega de paquetes, sin variar mucho su valor.

2.15.4. Análisis de la Cantidad de Paquetes para cada modelo

Cada modelo de propagación provoca un diferente comportamiento en la red, en lo referente a la producción de paquetes varía la cantidad que se generan; ya sean estos de datos, de control o de enrutamiento.

Es así que, mediante las simulaciones se pudo obtener los siguientes resultados que se expresan en la tabla 4.10 y que permiten apreciar como es la relación de la generación de paquetes en cada escenario, así como también los paquetes enviados y caídos.

Tabla 4.9. Cantidad de Paquetes para cada Modelo de Propagación

Modelo de Propagación Dos Rayos					
Densidad de Nodos	10	17	25	40	50
Paquetes Generados	2858	2678	2409	3252	2384
Paquetes Caídos	465	528	427	2035	4098
Paquetes AODV	898	1175	1261	2242	1958
Modelo de Propagación Free Space					
Densidad de Nodos	10	17	25	40	50
Paquetes Generados	6457	12472	4870	6313	4653
Paquetes Caídos	1414	3533	941	2736	1337
Paquetes AODV	2046	4621	1755	3596	2785
Modelo de Propagación Shadowing					
Densidad de Nodos	10	17	25	40	50
Paquetes Generados	2034	2141	2653	1775	1734
Paquetes Caídos	872	1540	3926	6190	10500
Paquetes AODV	1029	1310	1733	1398	1460

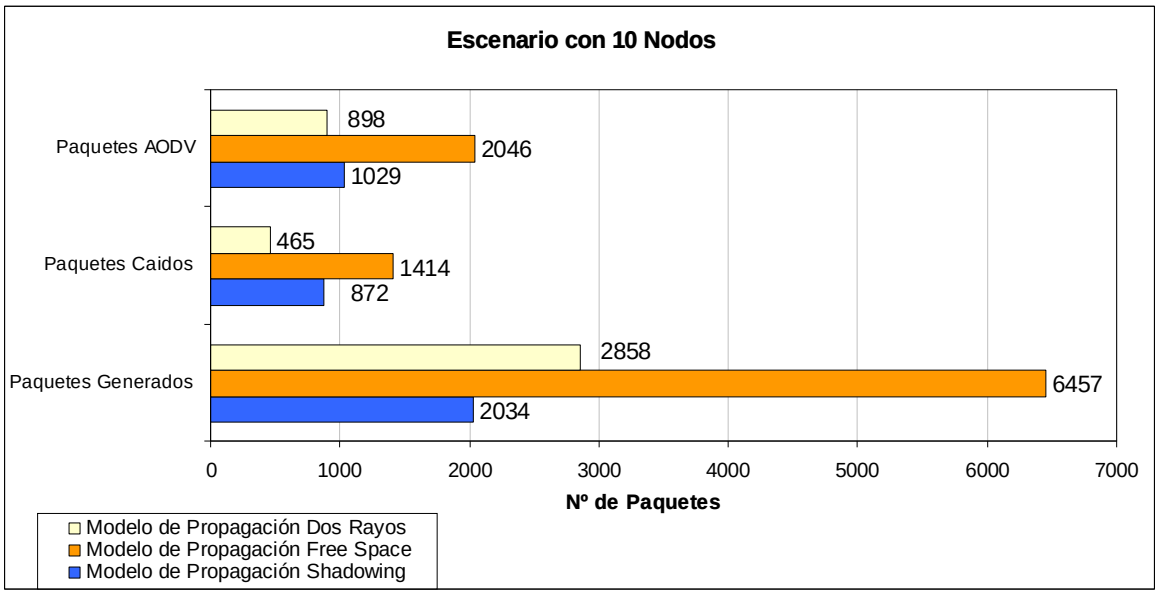


Figura. 4.16. Cantidad de paquetes para los escenarios de 10 Nodos

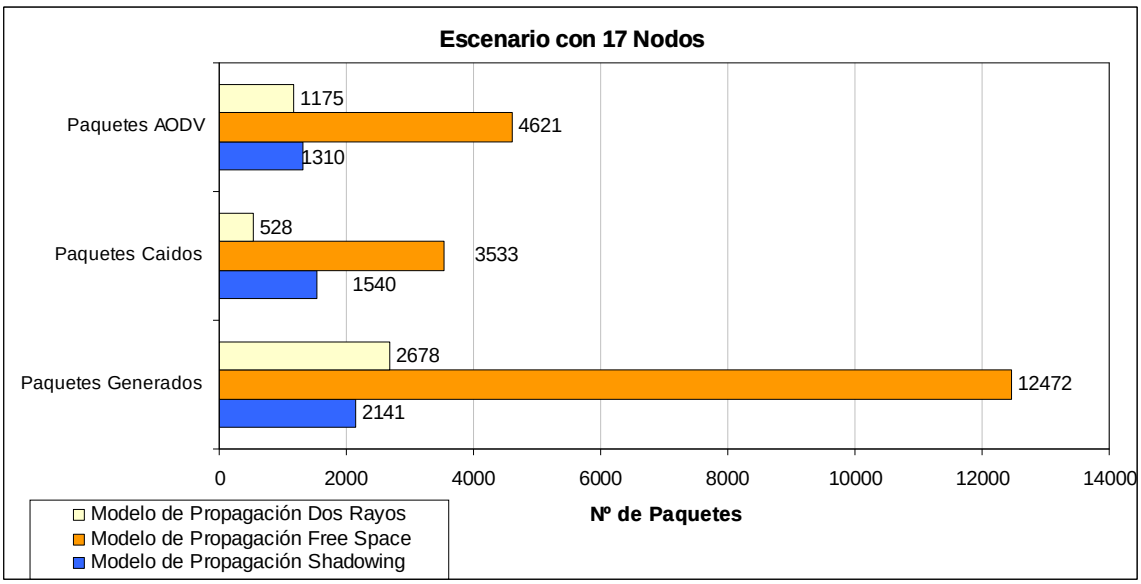


Figura. 4.17. Cantidad de paquetes para los escenarios de 17 Nodos

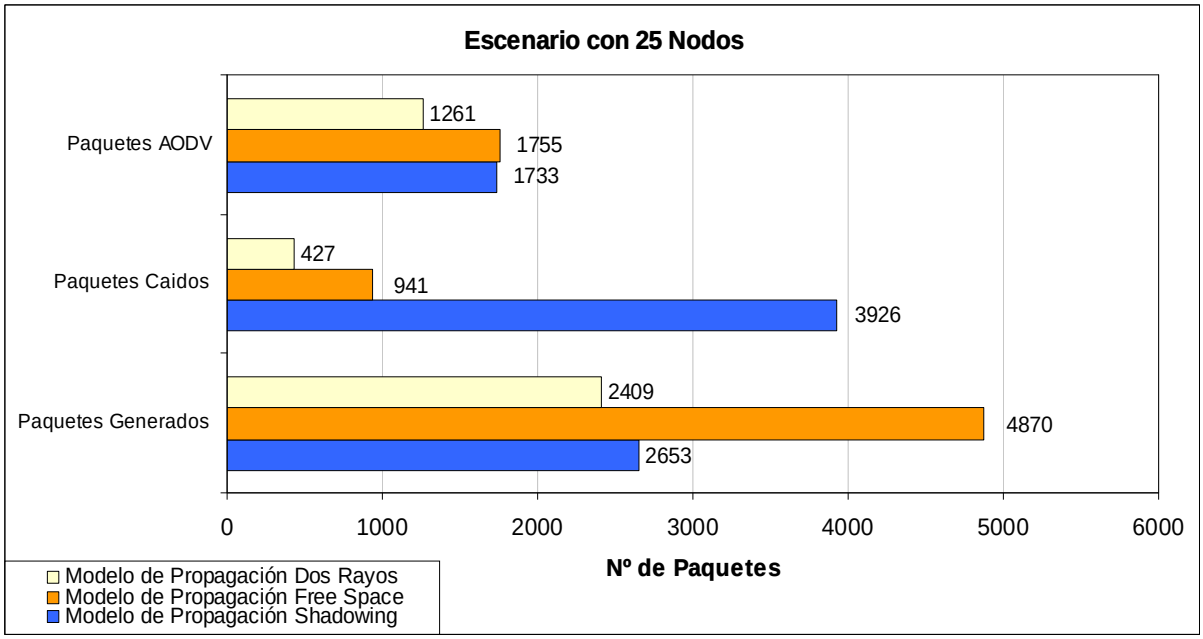


Figura. 4.18. Cantidad de paquetes para los escenarios de 25 Nodos

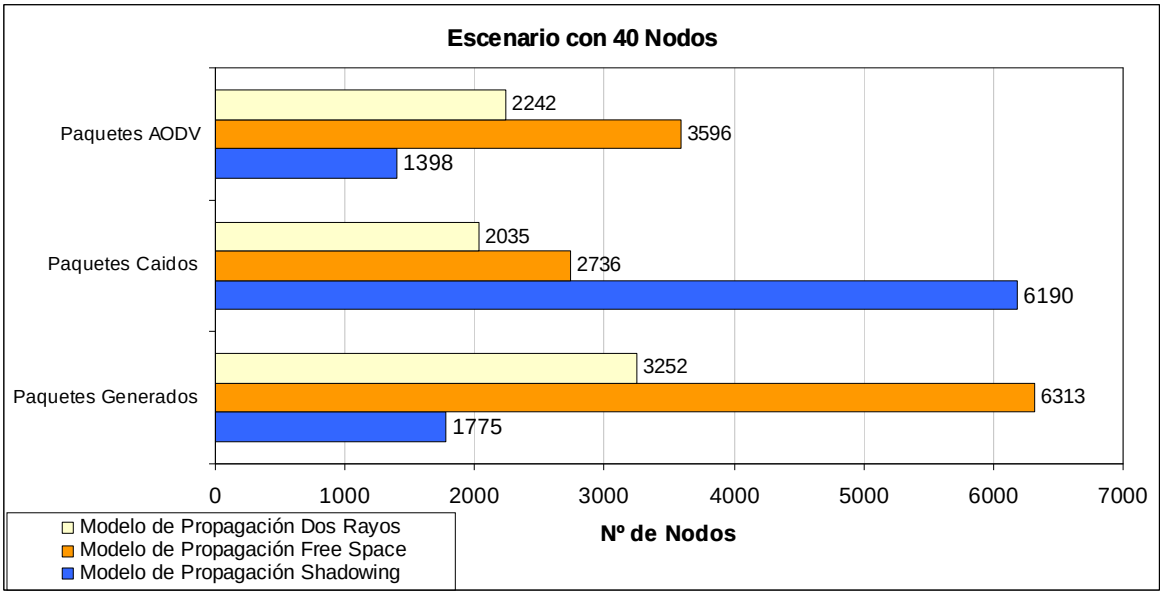


Figura. 4.19. Cantidad de paquetes para los escenarios de 40 Nodos

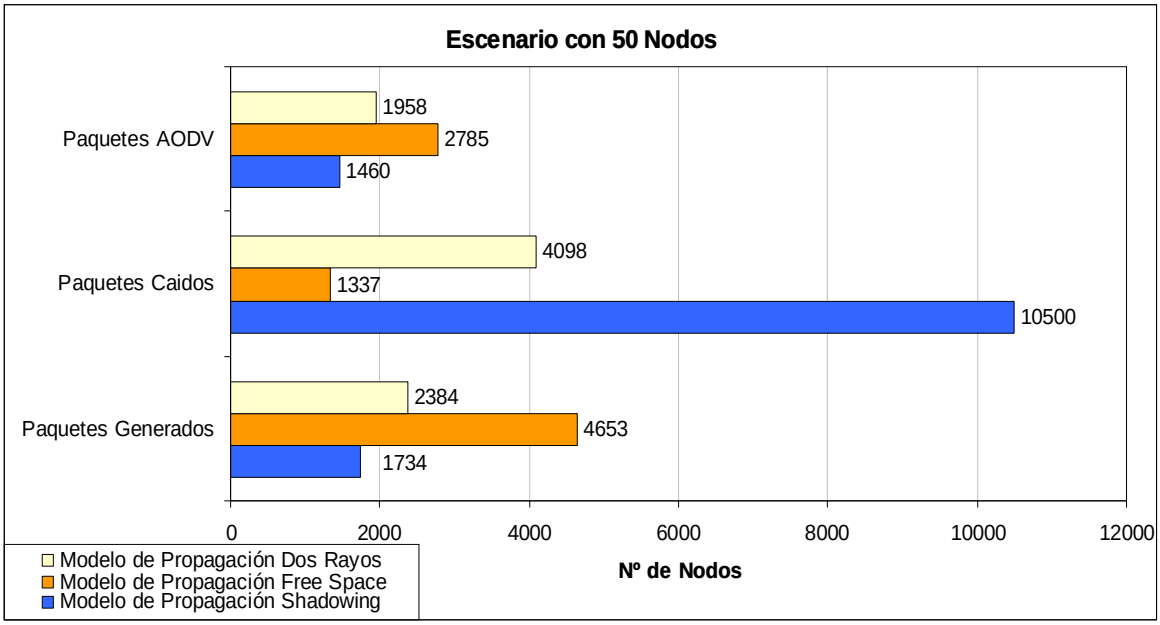


Figura. 4.20. Cantidad de paquetes para los escenarios de 40 Nodos

En las Figuras 4.16 a la 4.20 se puede distinguir como la cantidad de paquetes generados por el modelo de propagación Free Space siempre es mayor que cualquier otro modelo en cualquiera de los escenarios simulados, ya que no asume desvanecimientos ni perdidas por señales reflejadas en la tierra.

Para los cinco escenarios se puede observar que en todas las figuras los paquetes AODV relacionados al enrutamiento, representan una cantidad importante de los paquetes que se generan en la red, esto por la naturaleza misma del protocolo de enrutamiento que requiere periódicamente actualizar sus tablas, para lo cual realiza sus respectivas peticiones a sus vecinos.

De igual forma también, en todos los escenarios de simulación existen paquetes caídos que representan a los paquetes que los nodos desechan, ya sean porque son duplicados de otros, o porque no conocían la ruta para transmitirlos. Los paquetes caídos no necesariamente representan fallas en el envío desde el nodo origen hacia el nodo destino.

CAPÍTULO 5

Conclusiones y Recomendaciones

5.1. Conclusiones

- El modelo de propagación de Dos Rayos es considerado una mejora del modelo Free Space; sin embargo, para distancias cortas como es el caso de una WPAN, los dos modelos producen efectos muy similares en el comportamiento de la red
- El protocolo de enrutamiento AODV genera un consumo considerable de los recursos de red, ya que a pesar de ser un protocolo bajo demanda, cada cierto tiempo genera nuevos paquetes de enrutamiento para actualizar sus tablas, ingresando de esta forma mas tráfico a la red
- El Throughput o la capacidad de la red para manejar los paquetes que circulan en ella se decrementa al aumentar la densidad de nodos presentes en la red. La disminución de este parámetro se debe principalmente a que al existir mas nodos presentes en la red, aumenta el número de colisiones, provocando que los paquetes tengan que ser reenviados, generando de esta forma que un paquete sea efectivamente recibido en un mayor lapso de tiempo
- El parámetro Delivery Ratio o tasa de entrega de los paquetes de una red tiene un comportamiento similar al Throughput, es decir que al aumentar la cantidad de nodos este tiende a decrecer, reduciendo el porcentaje de entregas y recepciones efectivas.
- Asumir un modelo de propagación de Dos Rayos en una WPAN causa que el Throughput alcance los valores más altos en relación a los otros dos modelos, debido a que este modelo únicamente se ve afectado por

reflexiones de la señal en la Tierra, pero a cortas distancias esta consideración no es de gran relevancia.

- A pesar de que le modelo Free Space es considerado muy optimista y poco realista, para una WPAN sus resultados pueden ser considerados como validos, ya que las cortas distancias favorecen a que en realidad no afecten de gran manera los desvanecimientos y las ondas reflejadas en la superficie terrestre que asumen Shadowing y Dos Rayos respectivamente.
- El retardo en el tiempo de entrega de un paquete aumenta conforme también aumenta la densidad de nodos, debido a que existen mas rutas disponibles que pueden resultar ser ineficientes utilizando mayor cantidad de saltos en relación a otras rutas que se pueden calcular en el transcurso de la simulación; por lo que los paquetes enviados por rutas poco eficientes provocan que el tiempo de entrega se eleve. Esto ocurre principalmente por tipo de protocolo de enrutamiento que se está usando, ya que los paquetes AODV no conocen toda la ruta hacia el destino, únicamente conocen el siguiente salto, por lo que los primeros paquetes poseen una gran latencia.
- Las simulaciones en el programa NS-2.32 analizan varios parámetros que se los configura previamente para determinar el funcionamiento de una red, pero no se puede garantiza que los datos obtenidos sean completamente ciertos ni correctos, ya que para el estándar IEEE 802.15.4 recientemente se están creando y actualizando las librerías que permiten realizar las simulaciones, de hecho esta es la primera versión de Network Simulator que permite utilizar Zigbee, por lo que todavía faltan muchos aspectos por corregir.
- El estándar IEEE 802.15.4 presenta una limitación importante desde el punto de vista de protocolos de enrutamiento, ya que por el tamaño en bytes de sus paquetes, únicamente se puede usar AODV, o variaciones de otros protocolos conocidos, pero que no pueden ser configurados en NS-2.32

5.2. Recomendaciones

El desarrollo de este tipo de simulaciones genera expectativa en el verdadero rendimiento que puede llegar a tener una red WPAN basas en el estándar IEEE 802.15.4, por lo que sería recomendable que para futuros proyectos de grado, y con la colaboración de la ESPE, facilitando la adquisición de dispositivos que manejen esta tecnología, se pueda llegar a comprobar que tan acertados estaban los resultados obtenidos, en relación a la realización de pruebas de campo reales.

No se debe desestimar el uso del programa Network Simulator, que a nivel mundial es muy empleado tanto para la cátedra de Redes Inalámbricas, como para obtener datos muy precisos previos a la implementación de una red real. Por lo que sería de gran importancia que dentro del contenido de las asignaturas de programación o como una materia optativa se incluya el uso y desarrollo de esta herramienta, especialmente para la carrera de Electrónica en Redes y Telecomunicaciones.

REFERENCIAS BIBLIOGRÁFICAS CAPÍTULO 1

[1] Valle, Luís, Tesis Licenciatura Ingeniería en Electrónica y Comunicaciones, Universidad de las Américas Puebla, Coexistencia de Redes WLAN & WPAN, Capítulo 2.- WPAN Red Inalámbrica de Área Personal, http://catarina.udlap.mx/u_dl_a/tales/documentos/lem/valle_i_lf/capitulo2.pdf, pág. 2, May/2005.

[2] WPAN, http://searchmobilecomputing.techtarget.com/sDefinition/0,,sid40_gci837444,00.html, 14/Mar/2004

[3] IEEE 802.15, http://es.wikipedia.org/wiki/IEEE_802.15, 18/Oct/2007

[4] IEEE approves IEEE 802.15.1 standard for wireless personal area networks adapted from the bluetooth specification**,** http://standards.ieee.org/announcements/802151app.html

[5] IEEE 802.15.1 Document Information, http://electronics.ihs.com/documentt/abstract/OIHBIBAAAAAAAAAA

[6] IEEE P802.15 Wireless Personal Area Networks, http://grouper.ieee.org/groups/1451/5/Other%20Documents/IEEE%20802.15.4%20Interf%20desc.doc, Jul/ 2001

[8] Iglesias Yamilet, Hernández Dora, Introducción a las Redes Inalámbricas de Área Personal (WPAN), http://www.cujae.edu.cu/revistas/telematica/Articulos/422.htm, 6/Dic/2007

[9] IEEE 802.15 WPAN™ Task Group 3b (TG3b), http://www.ieee802.org/15/pub /TG3b.html

[10] IEEE 802.15 WPAN Millimeter Wave Alternative PHY Task Group 3c (TG3c), http://www.ieee802.org/15/pub/TG3c.html

[11] IEEE 802.15 WPAN Low Rate Alternative PHY Task Group 4a (TG4a), http://www.ieee802.org/15/pub/TG4a.html

[12] IEEE 802.15 WPAN™ Task Group 4b (TG4b), http://www.ieee802.org/15/pub /TG4b.html

[13] IEEE 802.15 WPAN™ Task Group 5 (TG5), http://www.ieee802.org/15/pub/TG5.html

[14] IEEE 802.15 WPAN™ Task Group 6 (TG6) Body Area Networks http://www.ieee802.org/15/pub/TG6.html

[15] Redes inalámbricas de área personal - WPAN, http://www.citel.oas.org/ne wsl etter/2006/enero/bluetooth_easp, Ene/2006

[16] Overby, Harald, IEEE 802.15, http://www.item.ntnu.no/fag/tm8100/Pensum stoff2004/IEEE%20802.15HARALD.ppt#275,25,IEEE 802.15.3 -QoS

[17] Vinagre, Juan José**,** LR-WPAN, htttp://www.tsc.urjc.es/investigacion/Seme narios_archivos/juanjo/802.15.4.ppt#280,1,Diapositiva 1, Nov/2004

REFERENCIAS BIBLIOGRÁFICAS CAPÍTULO 2

[19] ZigBee Tutorial, http://www.ifn.et.tu-dresden.de/~marandin/ZigBee/ZigBe eTutorial.html

[20] Wireless con ZigBee, http://netandtech.wordpress.com/zigbee/wireless-con-zigbee/, Abr/2007

[21] Martín, Javier - Ruiz, Daniel, Informe Técnico: ZigBee (IEEE 802.15.4), Universidad de Alicante, Departamento de Tecnología Informática y Computación, http://rua.ua.es:8080/bitstream/10045/1109/1/InformeTecZB.pdf, 26/Jun/2007

[22] NetAndTech, Wireless con ZigBee, http://netandtech.wordpress.com/zigbe e, Abr/2007

[23] IEEE Std 802.15.4™-2006, http://standards.ieee.org/getieee802/download/802.15.4-2006.pdf, Sep/06

[24] An implicit GTS allocation mechanism in IEEE 802.15.4 for time-sensitive wireless sensor networks: theory and practice http://portal.acm.org/citation.cfm?id=1348548&jmp=cit&coll=GUIDE&dl=

[25] ZigBee Alliance, ZigBee Specification – January 17, 2008

REFERENCIAS BIBLIOGRÁFICAS CAPÍTULO 3

[26] Virtual InterNetwork Testbed, http://www.isi.edu/nsnam/vint/index.

[27] Postigo, Marcos; Tesis Doctoral – Anexo A, Universidad Politécnica de Cataluña,2003; http://www.tdx.cat/TESIS_UPC/AVAILABLE/TDX-0508103-10394
7//TESIS.pdf

[28] Pérez, David; Tesis: Implementación de un modelo de canal inalámbrico para redes 802.11 bajo el simulador ns-2; Universidad Politécnica de Cataluña, Sep-2005

[29] Altam, Eintan; NS Simulator for Beginners; Dic-2003; http://www.sop.inria.fr/maestro/personnel/Eitan.Altman/COURS-NS/n3.pdf

[30] Roldán, Alfonso; Tesis: Estudio de modelos de movimiento en interiores para aplicación en entornos WLAN; Universidad Politécnica de Cataluña; Dic-2007; https://upcommons.upc.edu/pfc/bitstream/2099.1/4554/1/memoria.pdf

[31] Domingo, Mari Carmen; Tesis: Diseño y evaluación de un protocolo de descubrimiento de gateways para redes ad-hoc interconectadas a redes fijas; Universidad Politécnica de Cataluña; Jun 2006; https://upcommons.upc.edu/pfc/bitstream/2099.1/3752/1/53950-1.pdf

[32] Diapositivas: Redes y Servicios II: Practica 2. Simulación con NS; http://asignaturas.diatel.upm.es/rrss2/laboratorio/P2/2007-2008-P2-ns2-transparencias-apoyo-v1.pdf

[33] The VINT Project; The Ns Manual, Chapter 17 Ratio Propagation Models; Jun-2008; http://www.isi.edu/nsnam/ns/doc/ns_doc.pdf

[34] Subiela, Roberto; Simulación de protocolos de encaminamiento en redes móviles ad hoc con ns-2; http://w3.iec.csic.es/ursi/articulos_gandia_2005/articulos/TE2/396.pdf

[35] Departamento de Sistemas Telemáticos y Computación; Encaminamiento en Redes Ad-Hoc; Universidad Rey Juan Carlos; Nov-2007; http://gsyc.escet.urjc.es/moodle/file.php/27/Tansparencias_2007-08/encaminamiento-3.pdf

[36] Ortuño, Miguel Ángel, Protocolo de encaminamiento en origen con identificadores no únicos para redes Ad-Hoc de dispositivos con recursos limitados, Universidad Rey Juan Carlos; Jul-2006; http://eciencia.urjc.es/dspace/bitstream/10115/436/1/tesis.pdf

FECHA DE ENTREGA

El presente proyecto de grado fue entregado en la fecha.

Sangolquí, _____ 2009

Realizado por:

_____

Santiago Xavier Villacrés Torres

_____

Ing. Gonzalo Olmedo

COORDINADOR DE CARRERA DE TELECOMUNICACIONES