DEPARTAMENTO DE ELÉCTRICA Y ELECTRÓNICA

CARRERA DE INGENIERÍA EN ELECTRÓNICA Y TELECOMUNICACIONES

TRABAJO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN ELECTRÓNICA EN TELECOMUNICACIONES

TEMA: “DESARROLLO DE UNA NUEVA SOLUCIÓN PARA TCP INALÁMBRICO EN AMBIENTES DE LARGA DISTANCIA”

AUTOR: ARIAS IGUAGO MAURICIO ALEJANDRO

DIRECTOR: ING. LARA ROMÁN

SANGOLQUÍ

2016

UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

DEPARTAMENTO DE ELÉCTRICA Y ELECTRÓNICA

CARRERA DE INGENIERÍA EN ELECTRÓNICA EN TELECOMUNICACIONES

CERTIFICACIÓN

Certifico que el trabajo de titulación, "DESARROLLO DE UNA NUEVA SOLUCIÓN PARA TCP INALÁMBRICO EN AMBIENTES DE LARGA DISTANCIA" realizado por el señor MAURICIO ALEJANDRO ARIAS IGUAGO , ha sido revisado en su totalidad y analizado por el software antiplagio, el mismo cumple con los requisitos teóricos, científicos, técnicos, metodológicos y legales establecidos por la Universidad de Fuerzas Armadas ESPE, por lo tanto me permito acreditarlo y autorizar al señor MAURICIO ALEJANDRO ARIAS IGUAGO para que lo sustente públicamente.

Sangolquí, 29 de agosto de 2016

ING. ROMÁN LARA

ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

DEPARTAMENTO DE ELÉCTRICA Y ELECTRÓNICA

CARRERA DE INGENIERÍA EN ELECTRÓNICA Y TELECOMUNICACIONES

AUTORÍA DE RESPONSABILIDAD

Yo, ARIAS IGUAGO MAURICIO ALEJANDRO, con cédula de identidad N° 1716865595, declaro que este trabajo de titulación "DESARROLLO DE UNA NUEVA SOLUCIÓN PARA TCP INALÁMBRICO EN AMBIENTES DE LARGA DISTANCIA" ha sido desarrollado considerando los métodos de investigación existentes, así como también se ha respetado los derechos intelectuales de terceros considerándose en las citas bibliográficas.

Consecuentemente declaro que este trabajo es de mi autoría, en virtud de ello me declaro responsable del contenido, veracidad y alcance de la investigación mencionada.

Sangolquí, 11 de agosto de 2016

ARIAS IGUAGO MAURICIO ALEJANDRO

ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

DEPARTAMENTO DE ELÉCTRICA Y ELECTRÓNICA

CARRERA DE INGENIERÍA EN ELECTRÓNICA EN TELECOMUNICACIONES

AUTORIZACIÓN

Yo, ARIAS IGUAGO MAURICIO ALEJANDRO

Autorizo a la Universidad de las Fuerzas Armadas ESPE la publicación, en la biblioteca virtual de la Institución del trabajo "DESARROLLO DE UNA NUEVA SOLUCIÓN PARA TCP INALÁMBRICO EN AMBIENTES DE LARGA DISTANCIA", cuyo contenido, ideas y criterios son de mi exclusiva responsabilidad y autoría.

Sangolquí, 11 de agosto de 2016

ARIAS IGUAGO MAURICIO ALEJANDRO

DEDICATORIA

El presente trabajo de investigación está dedicado a mis familiares y amigos por su confianza, esfuerzo, cariño y buen ejemplo, al ayudarme a transitar por un camino de responsabilidad, honradez, por su ayuda incondicional a impulsar a alcanzar la meta profesional y por su inspiración para una superación constante.

AGRADECIMIENTO

Mis más sinceros agradecimientos a mis padres y hermanos por su apoyo y colaboración para hacer realidad el presente proyecto. A mis profesores, de manera especial al Ing. Román Lara director quien de manera desinteresada supo brindar su apoyo y consejos durante el desarrollo y culminación de este proyecto de investigación.

ÍNDICE DE CONTENIDOS

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

El presente proyecto va enfocado a encontrar la mejor solución para TCP inalámbrico en ambientes de larga distancia. A partir de varias soluciones como: *Delayed Duplicate Acknowledgments (DDA), Explicit Congestion Notification (ECN), Random Early Detection (RED), TCP modificado (incrementando el número necesario de ACK a 4, antes de reducir la ventana de transmisión).* Estas soluciones poseen características que ayudan a mejorar su desempeño en ambientes de larga distancia como son: diferenciación de paquetes perdidos por congestión o en el medio. También se comparó a varios simuladores capaces de realizar la simulaciones entre los cuales están: NCTuns, Network Simulator, OMNET, OPNET. Después de analizar las ventajas de cada uno de ellos como: la popularidad, facilidad de uso, cantidad de información entre otros aspectos, se escogió al simulador *Networwk Simulator 2,* el cual es uno de los simuladores más utilizados por investigadores y estudiantes, además de ser gratuito y si bien no posee una interfaz propia de visualización de resultados; posee aplicaciones externas fáciles de adquirir para la visualización de resultados. Cada solución se la simuló y analizó su comportamiento a varias distancias para poder visualizar el comportamiento de cada na a diferentes distancias. Conociendo las ventajas de cada una de las soluciones, la tasa de envío y su rendimiento es posible determinar la mejor solución que es la unión entre DDA y ECN.

Palabras Claves

- **DELAYED DUPLICATE ACKNOWLEDGMENTS (DDA)**
- **EXPLICIT CONGESTION NOTIFICATION (ECN)**
- ***RANDOM EARLY DETECTION (RED)***
- **NCTUNS**
- **NETWORK SIMULATOR**
- **OMNET**
- **OPNET**

ABSTRACT

This project is focused on finding the best solution for TCP in wireless long distance environments. From various solutions such as: Duplicate Delayed Acknowledgments (DDA), Explicit Congestion Notification (ECN), Random Early Detection (RED), TCP modified (increasing the required number of ACK to 4, before reducing the transmission window). These solutions have features that help to improve their performance in long distance environments such as: differentiation of congestion or packet loss in the environment. Also so many simulators were compared such as: NCTuns, Network Simulator, OMNET, OPNET. After analyzing the advantages of each of them as popularity, ease of use, amount of information, the simulator Networwk Simulator 2 were chosen, because it is one of the most used by researchers and students, also it is free and although it does not have an own interface display results; It has easy to acquire external applications for viewing results. Each solution was simulated and analyzed their behavior at various distances in order to visualize the behavior of each one at different distances. Knowing the advantages of each of the solutions, their rate and performance is possible to determine the best solution is the union between DDA and ECN.

Keywords

- **DELAYED DUPLICATE ACKNOWLEDGMENTS (DDA)**
- **EXPLICIT CONGESTION NOTIFICATION (ECN)**
- **RANDOM EARLY DETECTION (RED)**
- **NCTUNS**
- **NETWORK SIMULATOR**
- **OMNET**
- **OPNET**

CAPÍTULO I
INTRODUCCIÓN

1.1 Introducción a las comunicaciones inalámbricas de larga distancia

Wi-Fi (del inglés *Wireless Fidelity)* es una marca de la *Wi-Fi Alliance*, que ampara, prueba y certifica que los equipos cumplan con las normas 802.11, fue diseñada para redes de área local (LAN del inglés *Local Area Network*), su uso se ha extendido en países en vía de desarrollo hasta alcanzar enlaces de larga distancia.

Algunas empresas ven a WiFi de largo alcance como una posible solución para poder tener acceso a zonas, donde el acceso por satélite es muy caro y no es práctico llegar por cable, ya que muchas de estas zonas se encuentran en lugares que resultan inaccesibles. Mientras mayor sea la distancia de cobertura menor será la velocidad de transmisión sin embargo la velocidad es lo suficientemente alta para la transmisión correcta de datos.

Algunos radioaficionados han desarrollado enlaces de bajo costo llamadas *Paket Radio* en las bandas de Muy Alta Frecuencia (VHF del inglés *Very High Frequency*) y Alta frecuencia (HF del inglés *High Frequency*). Sin embargo las velocidades en las que trabajan son inferiores a las necesidades actuales.

Normalmente se coloca al nodo emisor en el borde de un área urbana, conectado a una Red de Área Local (LAN del inglés *Local Area Network*). Utilizando una antena direccional, con una ganancia alta, salen datos hacia una antena de recepción. La mayor distancia que se ha logrado crear una conexión ha sido de 382 km.

1.2 Wi-Fi de larga distancia

1.2.1 Historia

El nacimiento de Wi-Fi se dio gracias a la decisión tomada en 1985 por la Comisión Federal de Comunicaciones (FCC del inglés *Federal Communications Commission*) de abrir varias bandas de espectro inalámbrico, con el fin de utilizarlas sin necesidad de licencia o permiso del gobierno. Por lo que Michael Marcus tomo tres partes del espectro de las bandas médicas, industriales o científicas y las abrió a las comunicaciones inalámbricas.

Estas bandas denominadas bandas basura, (900MHz, 2.4GHz, 5.8GHz), eran ocupadas por otros instrumentos que tenían funciones diferentes de las comunicaciones como por ejemplo el horno de microondas. Así que la FCC abrió estas bandas para las comunicaciones con la condición de que cada equipo que utilice estas bandas, maneje y solucione por sí mismo las interferencias causadas por otros equipos. Lo que trajo el estudio de métodos que eviten o disminuyan al máximo las interferencias.

Inicialmente, los proveedores de equipos inalámbricos para redes de área local (LAN), como *Proxim* y *Symbol*, desarrollaron sus propios equipos para operar en las bandas sin licencia: por lo que el equipo de un vendedor no podía entenderse con el equipo de otro. Inspirados por el éxito de Ethernet, un estándar de redes, varios vendedores decidieron mantener un estándar inalámbrico común.

En 1988, *NCR Corporation*, que quería utilizar el espectro sin licencia para conectar cajas registradoras inalámbricas, preguntó a Victor Hayes, uno de sus ingenieros, para tratar de conseguir un estándar. Sr. Hayes, junto con Bruce Tuch de los Laboratorios Bell, se acercó al Instituto de Ingenieros Eléctricos y Electrónicos (IEEE del inglés *Institute of Electrical and Electronics Engineers*), donde un comité, denominado 802,3 ha definido el estándar Ethernet. Un nuevo comité denominado 802.11 se creó, con el Sr. Hayes como presidente, y comenzó las negociaciones.

Un mercado fraccionado hizo que pasara mucho tiempo la aceptación del estándar por varios vendedores de equipos. En 1997, la comisión aprobó un pliego de condiciones. Se permitió una tasa de transferencia de datos de 2 Mbps, utilizando cualquiera de las dos tecnologías *spread spectrum*, salto de frecuencia o la transmisión directa de secuencia. (La primera evita la interferencia de otras señales, saltando entre las frecuencias de radio, y el segundo se propaga la señal a lo largo de una banda ancha de frecuencias).

El enorme éxito de Wi-Fi en todos los ámbitos ha dado lugar a una gran cantidad de productos en el mercado, casi todos ellos de bajo consumo, a precios bajos y mucha flexibilidad de uso. Respetando la máxima potencia transmisible en 2.4 GHz establecida en cada país.

La Tabla 1 muestra la potencia máxima que es permitida en las diferentes regiones del planeta mientras la Tabla 2 muestra las ventajas y desventajas de usar Wifi de largas distancias (Wild del inglés WiFi-based Long Distance).

Tabla. 1

Máxima potencia transmisible en 2.4 GHz por regiones.

Máxima potencia Transmisible	Lugares
1 W.	Estados Unidos y países en desarrollo
100 mW.	Europa
10 mW.	Japón

Fuente: (Kioskea.net, 2014)

Tabla. 2

Ventajas y Desventajas de *Wild* Wi-Fi.

Ventajas	Desventajas
Frecuencias sin licencia (2.4 / 5.8 GHz) con limitaciones de potencia.	Se necesita línea de vista directa
Velocidades (1 - 54 Mbps), su *throughput* neto (50-70%)	Fue construida para trabajar en distancias cortas, por lo que es necesario resolver algunos problemas a la hora de utilizar en distancias de decenas de kilómetros
Tecnología con estándar ampliamente conocido y fácil de configurar, bajos costos en equipos.	Mientras la cantidad de usuarios aumenta, también lo hace la cantidad de colisiones.
Bajo consumo de potencia.	Poseen tan solo 3 canales en 2.4 GHz y 8 en 5.8 GHz que no se interfieren entre sí.
Flexibilidad: Permite crear cambios en la red fácilmente debido a la facilidad para que un nodo se adhiera a otro.	
Gran resistencia contra condiciones meteorológicas adversas.	

Fuente: (Kioskea.net, 2014)

1.2.2 Conceptos y Definiciones

Wi-Fi

Wi-Fi es el nombre de la certificación entregada por la Wi-Fi Alliance, cuando los equipos cumplen con las normativas del estándar 802.11. Por motivos de marketing, desconocimiento de las personas que hacen mal uso del nombre del estándar se confunde con el nombre de la certificación. Una red Wi-Fi es en realidad una red que cumple con el estándar 802.11. Los dispositivos certificados por Wi-Fi *Alliance* se les permite usar este logotipo (Figura 1).

Figura 1: Logotipo de la alianza Wi-Fi

Debido a que datos se transmiten sin cables no es posible conocer cuando se producen colisiones por lo que no es necesario detectar la colisión sino evitarla. Por esto se utiliza el método Acceso Múltiple con escucha de portadora y anulación de colisiones (CSMA/CA del inglés *Carrier Sense Multiple Access with collision avoidance*) en lugar del que utilizan las conexiones cableadas que es: Acceso múltiple con escucha de portadora y detección de colisiones (CSMA/CD del inglés *Carrier Sense Multiple Access with Collision Detection*).

Estándares Wi-Fi

La familia de estándares IEEE 802.11 (802.11a, 802.11b, 802.11g, 802.11n), tienen asignadas las bandas ISM (Industriales, Científicas y Médicas del inglés *Industrial, Scientific and Medical*) 902-928 MHz, 2.400-2.4835 GHz, 5.725-5.850 GHz. A continuación presentaremos las características de cada una.

802.11a

Está fundamentado en la tecnología llamada multiplexación por división de frecuencias ortogonales (OFDM del inglés *Orthogonal Frequency Division Multiplexing*). Utiliza la banda de 5 GHz con 8 canales no superpuestos siendo incompatibles con los dispositivos 802.11b. Existen dispositivos denominados “banda dual” que pueden comunicarse tanto con el estándar 802.11 a como con el 802.11b. La Tabla 3 muestra las velocidades hipotéticas del estándar en ambientes cerrados a diferentes distancias.

Tabla. 3

Velocidad hipotética (en ambientes cerrados).

Velocidad hipotética (en ambientes cerrados)	Distancia
54 Mbps	10 m
48 Mbps	17 m
36 Mbps	25 m
24 Mbps	30 m
12 Mbps	50 m
06 Mbps	70 m

Fuente: (Kioskea.net, 2014)

802.11b

El estándar 802.11b tiene una tasa de transferencia de 11 Mbps en un rango aproximado de 100 metros en ambientes cerrados y de más de 200 metros al aire libre (con antenas direccionales). Utiliza la banda de 2.4 GHz. Si quitamos la cabecera de CSMA/CA la tasa máxima de 802.11b es de 5.9Mbps usando TCP y 7.1 usando UDP. A continuación tenemos la Tabla 4 que muestra las velocidades hipotéticas que alcanzaría este estándar a diferentes distancias.

Tabla. 4

Velocidad hipotética en ambientes cerrados y abiertos.

Velocidad hipotética	Distancia (en ambientes cerrados)	Distancia (al aire libre)
11 Mbps	50 m	200 m
5,5 Mbps	75 m	300 m
2 Mbps	100 m	400 m
1 Mbps	150 m	500 m

802.11g

Posee una tasa transferencia de datos máxima de 54 Mbps. Es compatible con los dispositivos del estándar 802.11b. A continuación tenemos la Tabla 5 que muestra las velocidades hipotéticas que alcanzaría este estándar a diferentes distancias.

Tabla. 5

Velocidad hipotética en ambientes cerrados y abiertos.

Velocidad hipotética	Distancia (en ambientes cerrados)	Distancia (al aire libre)
54 Mbps	27 m	75 m
48 Mbps	29 m	100 m
36 Mbps	30 m	120 m
24 Mbps	42 m	140 m
18 Mbps	55 m	180 m
12 Mbps	64 m	250 m
09 Mbps	75 m	350 m
06 Mbps	90 m	400 m

Fuente: (Kioskea.net, 2014)

802.11n

Se basa en la tecnología Múltiple Entrada Múltiple Salida (MIMO del inglés *Multiple input Multiple output)*. Las ondas de Radio Frecuencia (RF del inglés Radio Frequency) son "Multi-Señal" y siempre existe una onda primaria y varias secundarias. Utiliza ambas bandas de frecuencia simultáneamente 2.4GHz y 5 GHz. La Tabla 6 muestra un resumen de los estándares de la familia de estándares IEEE 802.11.

Tabla. 6

Resumen de Estándares Wi-Fi.

Estándar	Nombre	Descripción
802.11a	Wi-Fi5	Velocidad Teórica 54 Mbps Velocidad Real 30 Mbps. Banda 5 GHz.
802.11b	Wi-Fi	Velocidad Teórica de 11 Mbps Velocidad Real 6 Mbps Banda 2.4 GHz.
802.11e	Mejora de QOS	Mejora del estándar se le incluye calidad de servicio para mejorar su rendimiento.
802.11g		Ofrece un ancho de banda elevado (con un rendimiento máximo de 54 Mbps, de 30 Mbps en la realidad) en el rango de frecuencia de 2,4 GHz. El estándar 802.11g es compatible con el estándar 802.11b.
802.11i		Mejora de Seguridad

1.2.3 Dificultades al utilizar de Wi-Fi en ambientes de largas distancias

Al inicio Wi-Fi fue diseñada para redes pequeñas, se debe realizar pequeños cambios para solventar los problemas al utilizarla en largas distancias

Capa Física

No existe ningún elemento de la capa física que determine el alcance de las comunicaciones Wi-Fi. La distancia que podrá ser alcanzada dependerá delos siguientes parámetros:

- PIRE Potencia Isotrópica Radiada Equivalente, que es la cantidad de potencia que podamos emitir
- Las pérdidas en el medio.
- La sensibilidad de la antena receptora.

.**Velocidad**

El protocolo IEEE 802.11 recoge distintas velocidades según el modo de funcionamiento. Estos modos usan diferentes tipos de modulación y codificación; conociendo que si necesitamos una mayor velocidad también necesitaremos de una mayor potencia para mantener una Tasa de Error Binario (BER del inglés Bit Error Rate) baja; por tanto, es mejor usar velocidades bajas para mantener estables los enlaces de larga distancia.

Fenómenos meteorológicos.

Existen varios problemas ocasionados por las condiciones meteorológicas adversas. Entre ellas la lluvia que puede no solo empeorar la comunicación sino que también afecta a los equipos si no se encuentran protegidos correctamente y si bien los estudios muestran que las nubes o la niebla no perjudican en gran manera, todo dependerá de la distancia del enlace.

Interferencias.

Esto no es un problema común en zonas rurales aisladas; sin embargo, siempre es un problema a solventar cuando se realizan enlaces.

Capa MAC

Aquí el problema se presenta en los tiempos constantes definidos en tres tipos de temporizadores de espera de los ACKs que son:

ACKtimeout

El tiempo en que el nodo receptor espera a los ACK antes de determinar al paquete como perdido. Para que el enlace Wi-Fi funcione es necesario que el *ACKtimeout* sea mayor que el tiempo de propagación de ida y vuelta más el Pequeño Espacio Entre tramas (SIFS del inglés *Short Interframe Space*).

Si una estación está muy lejos como para recibir el ACK antes de que termine el *ACKtimeout*, se interpretará que el paquete se perdió y se retransmitirá. La estación transmisora pensará que el paquete no pudo llegar, aún si este llego sin problemas.

Slottime

Los valores de Slottime, SIFS y DIFS tienen un límite de unos 3 km. después de eso las calidad del enlace empiece a decrecer.

La Figura 2 muestra el diagrama de Slottime y el orden de activación en la transmisión de paquetes mientras que La Tabla 7 muestra los valores de slottime para cada estándar

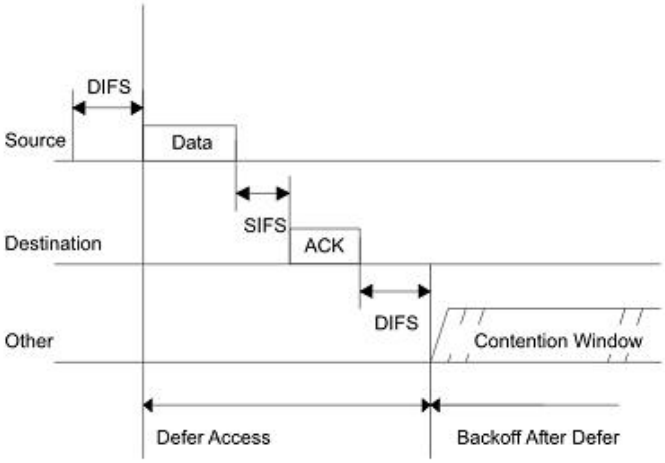


Figura 2 Diagrama de Slottime.

Fuente (Wireless QoS, 2010)

Tabla. 7

Valores de Slottime de cada estándar.

802.11b	
Slottime	20 µs
SIFS	10 µs
PIFS	SIFS + Slottime = 30 µs
DIFS	SIFS + 2 Slottime = 50 µs
802.11g	
Slottime	9 µs
SIFS	10 µs
DIFS	SIFS + 2 Slottime = 28 µs
802.11 a	
Slottime	9 µs
SIFS	16 µs
DIFS	SIFS + 2 Slottime = 34 µs

Fuente: (Ermanno, 2007)

La vulnerabilidad con nodos ocultos.

Se considera como “nodo oculto” a la situación donde no todas las estaciones pueden escucharse, Dicho problema ocurre cuando dos terminales, que están fuera de sus respectivas áreas de cobertura, transmiten simultáneamente a un mismo terminal, que pertenece al área de cobertura común de los dos transmisores, produciéndose una colisión en dicho receptor, que no es detectada por los transmisores.

En IEEE 802.11 se emplea el mecanismo “Preguntar si enviar / Libre para enviar” (RTS/CTS del inglés *Request to Send / Clear to Send*) para evitar colisiones entre nodos ocultos, mientras la distancia aumenta, su efectividad disminuye; en enlaces Punto-Multipunto con enlaces a largas distancias,el RTS/CTS no funciona correctamente.

En la Figura 3 podemos observar el problema del nodo oculto donde tenemos tres equipos. El equipo B (Rango de transmisión color verde) Puede observar tanto al equipo A (Rango de transmisión azul) como a C (rango de transmisión rojo); sin embargo el equipo A no puede observar al equipo C ni viceversa por lo que el equipo A no puede saber el momento en que el equipo C esté transmitiendo hacia el equipo B.

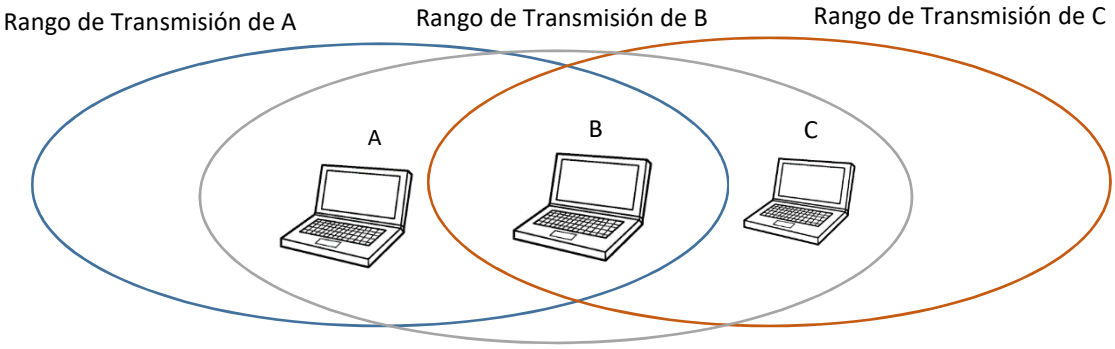


Figura 3 Nodo Oculto.

1.2.4 Perdidas

La cantidad de señal que se pierde al atravesar el medio al realizar un enlace.

Por Desvanecimiento

Un desvanecimiento es se produce cuando la señal se atenúa, pierde potencia, en el espacio debido a obstáculos y la resistencia que debe traspasar hasta llegar a su destino. Se debe normalmente a los cambios atmosféricos y a las reflexiones del trayecto de propagación al encontrar superficies terrestres o acuáticas.

- **Desvanecimiento plano**, cuando afecta por igual a todas las componentes de la señal, el desvanecimiento es uniforme y la señal no sufre grandes deformaciones.
- **Desvanecimiento Selectivo**, cuando éste se produce en una zona del espectro de la señal transmitida, afectando a un margen pequeño de frecuencias.
- **Desvanecimiento Compuesto**, es el resultado de la suma de los efectos del desvanecimiento plano y selectivo.

Por Obstáculos

Obstáculos que entorpecen la visión (los valores en dB de pérdidas variarán en función de los materiales y grosor del obstáculo) La señal inalámbrica va perdiendo potencia a medida que se propaga y va traspasando obstáculos. Debido a que se transmite energía y esta es absorbida por los objetos (paredes, muebles metálicos, etc.) que encuentra a su paso.

Los obstáculos producen la reflexión y la difracción de la señal.

REFLEXIÓN

Cuando un rayo incide sobre una superficie pulida y lisa y rebota hacia el mismo medio decimos que se refleja y cumple las llamadas "leyes de la reflexión"

- El rayo incidente forma con la normal un ángulo de incidencia que es igual al ángulo que forma el rayo reflejado y la normal, que se llama ángulo reflejado.

- El rayo incidente, el reflejado y la normal están en el mismo plano. (Si el rayo incidente se acerca al 2º medio en el plano del papel, el reflejado estará en ese plano y no se irá ni hacia adelante ni hacia atrás).

REFRACCIÓN

Se dice que un rayo se refracta (cambia de dirección) cuando pasa de un medio a otro en el que viaja con distinta velocidad. En la refracción se cumplen las siguientes leyes:

- El rayo incidente, el refractado y la normal están en el mismo plano.
- Se cumple la ley de Snell

Las pérdidas por difracción por obstáculos aislados son estimadas utilizando el modelo de “filo de cuchillo” de Fresnel-Kirchoff. La Figura 4 muestra el comportamiento de reflexión y refracción de una onda al chocar con un medio diferente

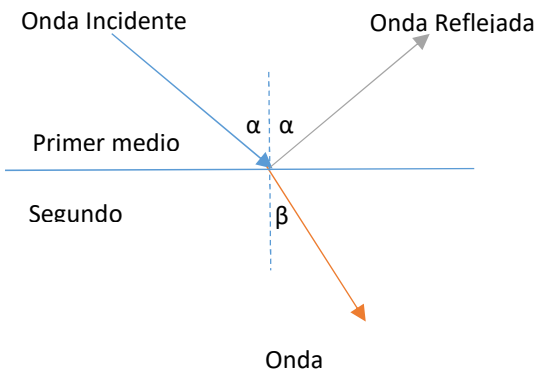


Figura 4 Reflexión y Refracción.

Por Ruido

Son señales que interfieren en la transmisión en los enlace y sobre las cuales no se puede tener un completo control. Es el resultado de diversos tipos de perturbación que ocasiona que produzcan errores en los enlaces.

El ruido se produce por el uso de componentes electrónicos en especial amplificadores, ruido térmico de las resistencias, interferencias de señales externas, etc. Sin importar lo que hagamos no es posible quitar el ruido completamente. Sin embargo podemos limitarlo para mantener un buen enlace.

El ruido se clasifica dependiendo de su origen. Si el ruido proviene de los elementos del sistema se conoce como “ruido interno”. Caso contrario se denomina el “ruido externo”. El ruido se clasifica en:

- **Ruido Atmosférico**. Al ruido producido por el medio ambiente lluvias, rayos, neblinas. etc.
- **Ruido Extraterrestre**. Ruidos causados por elementos que se encuentran fuera del planeta ya como tormentas solares y radiaciones causados por algunas estrellas.
- **Ruido producido por el hombre**. El ruido causado por instrumentos creados por el hombre como lámparas fluorescentes.

´1.2.4. Por Interferencia de canal

Por interferencia se entiende que en el receptor, junto a la señal útil, se presenta una señal indeseada que corresponde a otra comunicación y que tiende a degradar y dificultar la recepción de la señal de interés. Se distingue entre:

Interferencia cocanal.

Es una interferencia que se presenta en la misma banda de frecuencias que la señal útil. Se presenta debido a la energía fácilmente detectada entre dos canales adyacentes.

Se da cuando Puntos de Acceso (AP del inglés *Access Points),* cuyas áreas de cobertura se superponen, están configurados en el mismo canal o en canales solapables, esto conlleva a problemas de conectividad en los clientes que se encuentran en áreas de cobertura superpuesta. Esto se muestra en la Figura 5. Para evitar este tipo de problemas, se debe cambiar el canal actual hacia uno no solapable, o mueva el *AP* hacia un lugar más lejano de tal forma que las áreas de cobertura no se superpongan.

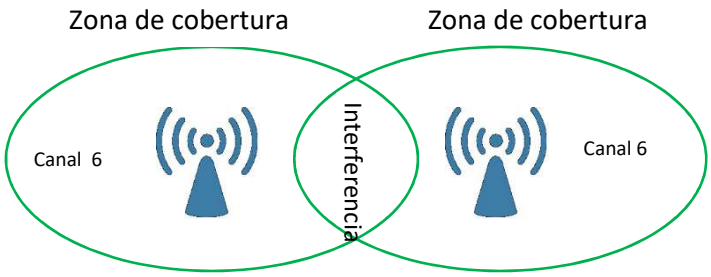


Figura 5 Esquema de evaluación de interferencia de canal adyacente.

Interferencia de canal adyacente.

Es una interferencia que se presenta por una señal en una banda distinta a la de la señal útil.

Se da cuando los *AP* están localizados muy cerca uno del otro o se usan valores muy altos de potencia RF (Radiofrecuencia), esto causa interferencia, aun cuando los *AP* están configurados en canales no solapables. Para evitar este tipo de problemas. Disminuya la potencia RF (Radiofrecuencia) de su *AP* para arreglar este problema. Las interferencias más perjudiciales son las cocanal, ya que las de canal adyacente pueden, en general, eliminarse o reducirse con la propia selectividad del transmisor y del receptor.

1.2.5 Importancia

Tiene una gran importancia en el ámbito económico, social y científico de una ciudad ya que es un recurso muy utilizado en hoteles, universidades, para llegar a zonas de difícil acceso, y en otros usos

Social

Wi-Fi tiene una gran importancia ya que actualmente todavía existen regiones en varias partes del mundo que aún no acceden a servicios de comunicaciones de banda ancha. Una de las razones es debido a las zonas geográficas. Es por eso que las tecnologías inalámbricas como Wi-Fi se han convertido en una pieza clave para dotar de servicios de ancho de banda a localizaciones donde la penetración de infraestructuras de telecomunicaciones no es rentable desde el punto de vista económico.

Universidades

La cobertura de la red inalámbrica alcanza zonas comunes como bibliotecas, cafeterías, salas de conferencias, zonas exteriores, laboratorios etc. En todas ellas los alumnos que dispongan de un ordenador portátil, PDA u otro terminal inalámbrico son capaces de acceder a información sobre el campus, horarios de exámenes, de clases, profesorado, así como a ejercicios, prácticas, consultas a profesores, aplicaciones de e-learning etc.

Hoteles

Wi-Fi representa un valor añadido que el hotel puede ofertar a sus clientes, ya que hace posible la conexión inalámbrica a Internet desde las habitaciones y espacios comunes. Se trata de un servicio que puede llegar a ser diferenciador a la hora de contratar un hotel, puesto que los profesionales y gente de negocios eligen hoteles con conexión a Internet y a ser posible Wi-Fi.

CAPÍTULO II
PROTOCOLO TCP

2.1 Protocolo TCP

Protocolo de Control de Transmisión (TCP del inglés *Transmission Control Protocol*), está pensado para ser utilizado como un protocolo *"host"* a *"host"* muy fiable entre miembros de redes de comunicación de computadoras por intercambio de paquetes. Controla la división de la información en unidades individuales de datos (llamadas paquetes) para que estos sean encaminados eficientemente hacia su punto de destino.

TCP divide el flujo de bytes en segmentos de tamaño apropiado (esta limitación viene impuesta por la unidad máxima de transferencia (MTU del inglés *Maximum Transmission Unit*). Entonces, TCP pasa el segmento resultante a la capa IP (Protocolo de Internet del inglés *Internet Protocol*), donde luego de atravesar la red, llega a la capa TCP de la entidad destino. Este comprueba que ningún paquete se haya perdido y que hayan llegado ordenados.

Establecimiento de una conexión

Es necesario que ambas máquinas se sincronicen utilizando la negociación en tres pasos, también utilizada al cierre de la sesión. Posibilita el inicio de la comunicación en tres etapas.

- Primero, el emisor o cliente transmite un segmento con el indicador SYN está fijado en 1 y con número de secuencia N denominado número de secuencia inicial del cliente (Figura 6).

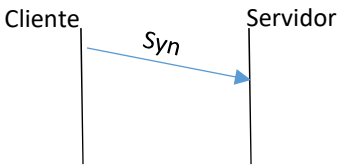


Figura 6 Primera etapa del establecimiento de una conexión TCP

- Después el receptor o también llamado servidor recibe el paquete inicial, entonces envía un acuse de recibo, un segmento en el que el indicador ACK está fijado en 1 y el indicador SYN está fijado en 1. Incluye el número del servidor (el número de secuencia inicial para el cliente). El acuse de recibo que contiene el número de secuencia inicial del cliente incrementado en 1 (Figura 7).

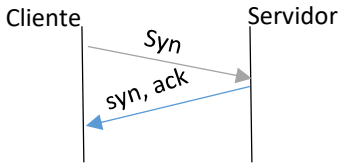


Figura 7 Segunda etapa del establecimiento de una conexión TCP

- Por último, el cliente wnvía un acuse de recibo, con indicador ACK en 1 y el indicador SYN está fijado en 0. Su número de secuencia está incrementado y el acuse de recibo representa el número de secuencia inicial del servidor incrementado en 1 (Figura 8).

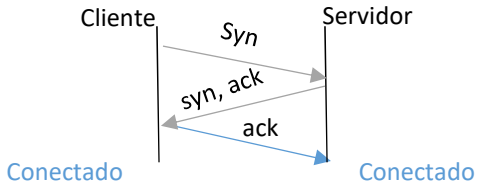


Figura 8 Etapa final del establecimiento de una conexión TCP

Una vez realizado este procedimiento se sincronizó las dos máquinas y puede comenzar la comunicación entre ellas.

Finalización de la conexión

Tanto el servidor como el cliente pueden cerrar la comunicación. Para lo cual se procede de la siguiente manera:

- La máquina que quiera finalizar la comunicación envía un segmento con el indicador FIN fijado en 1, para colocarse en estado de espera.
- Después la otra máquina envía un acuse de recibo con el indicador FIN fijado en 1 y sigue enviando los segmentos en curso.
- Finalmente la máquina informa a la aplicación la comunicación se acabó y luego envía un segmento FIN a la otra máquina, cerrando la conexión.

2.1.1 Historia

A principios de los 60, se necesitaba compartir recursos informáticos de una manera más rápida y eficiente. En 1961, se introduce el término de Conmutación de Paquetes (*Packet Switching*) por Leonard Klienrock. Con el fin de que comunicación entre máquinas fuese dividida en paquetes. Si cada paquete contenía su dirección de salida como de destino podría encontrar por sí mismo el camino para atravesar la red.

En 1969 la Agencia de Proyectos de Investigación Avanzada (*Defense Advanced Research Projects Agency* o DARPA) del Ejército de los EEUU desarrolla la ARPAnet. Aunque dicha red funcionaba bien, estaba sujeta a algunas caídas periódicas del sistema. Por lo que en 1974 V. Cerf y R. Kahn propusieron un nuevo conjunto de protocolos básicos de red que solventaban gran parte de los problemas de los protocolos usados en ARPANET. Así se pusieron los cimientos de los protocolos IP (*Internet Protocol*) y TCP (*Transmission Control Protocol*).

En 1980 se comenzó la migración de los aproximadamente 100 servidores que formaban la red ARPANET a los nuevos protocolos. En 1983 el Departamento de Defensa estandarizó el protocolo TCP/IP como protocolo básico de red.

2.1.2 Conceptos y Definiciones

Formato de los segmentos TCP

Se encuentra en la capa transporte, los paquetes se envían en forma de "segmentos". El formato de los segmentos TCP se muestra en el siguiente esquema:

Figura 9 Esquema del segmento TCP

Cada segmento TCP está constituido por las siguientes partes:

- **Puerto de origen (16 bits):** Identifica el puerto del emisor
- **Puerto destino (16 bits):** Identifica el puerto del receptor.
- **Número de secuencia (32 bits):** Comprueba que ningún segmento se ha perdido, y que llegan en el orden correcto.

- **Número de acuse de recibo (ACK) (32 bits):** Contiene el número de secuencia del siguiente paquete que el receptor espera recibir.
- **Longitud de la cabecera TCP (4 bits):**
- **Reservado (4 bits):** Bits reservados.
- **Bits de control (flags) (8 bits):** Son 8 *flags* o banderas. Cada una indica “activa” con un 1 o “inactiva” con un 0.

    - **CWR o “*Congestion Window Reduced*” (1 bit):** Muestra si se ha recibido un paquete TCP con el *flag* ECE activado.

    - **ECE o “*ECN-Echo*” (1 bit):** Indica que el receptor puede realizar notificaciones ECN.

    - **URG o “*urgent*” (1 bit):** Si se encuentra activo significa que el campo “Urgente” es importante.

    - **ACK o “*acknowledge*” (1 bit):** Ayuda a determinar si el paquete enviado llego correctamente a su destino.

    - **PSH o “*push*” (1 bit, ver PSH):** Activa o desactiva que los datos de este segmento y los que hayan sido almacenados anteriormente en el buffer del receptor deben ser transferidos a la aplicación receptora lo antes posible.

    - **RST o “*reset*” (1 bit):** Termina la conexión sin esperar respuesta.

    - **SYN o “*synchronize*” (1 bit):** Activa/desactiva la sincronización de los números de secuencia.

    - **FIN (1 bit):** Finaliza la conexión.

- **Ventana (16 bits):** Especifica el número de bytes que el receptor está actualmente esperando recibir.

- **Suma de verificación (*checksum*) (16 bits):** Verifica si existe errores en los datos recibidos.
- **Puntero urgente (16 bits):** Si el *flag* URG está activado, entonces este campo indica el desplazamiento respecto al número de secuencia que indica el último byte de datos marcados como "urgentes".
- **Opciones (número de bits variable):** La longitud total del campo de opciones ha de ser múltiplo de una palabra de 32 bits (si es menor, se ha de rellenar al múltiplo más cercano).
- **Datos (número de bits variable):** No forma parte de la cabecera, es la carga (*payload*), la parte con los datos del paquete TCP.

Congestión de red

Congestión es exceso de tráfico en alguna parte de la red. Causando problemas en los enlaces. Si un nodo sufre este problema y no se solucione puede provocar el fallo de toda la red. Las consecuencias causadas por la congestión son: Retardos, pérdidas, desperdicios de recursos ocasionados al realizar retransmisiones innecesarias ya que grandes retardos ocasionan que venzan los temporizadores de retransmisión antes que llegue la confirmación de los mensajes enviados (ACK), ocasionando que el ancho de banda de los enlaces sea utilizado para enviar copias de los paquetes que no son necesarias.

Dinámica del control de la congestión

Los mecanismos de control de congestión, pueden ser:

Preventivos (**lazo abierto)**.

- Control de admisión: Controlando la cantidad de usuarios.
- Monitorización: Controlando un flujo no exceda su un límite de tráfico.
- Regulación de tráfico: Cambiando el patrón de tráfico a la entrada consiguiendo que el tráfico sea más predecible.

Reactivos (**lazo cerrado o con realimentación**).

- **Realimentación directa**: Los nodos de conmutación envían paquetes especiales a los nodos extremos informando si existe peligro de congestión o si ya se produjo una.
- **Realimentación indirecta:** Los extremos analizan la existencia de retardos y pérdidas para determinar que existe congestión

Soluciones de TCP para la congestión

Fue introducido por Van Jacobson. Con el fin de que el emisor conozca la cantidad de paquetes que debe transmitir en cada momento. Para lo cual se introdujo la ventana de control de flujo, *RcvWindow*, la ventana de control de congestión, *CongWindow*.

La ventana de congestión, y la tasa de transmisión, se incrementa cuando el emisor recibe las confirmaciones; Sin embargo cuando detecta una pérdida, la ventana de congestión se decrementa. El algoritmo de control de congestión de TCP consta de tres componentes principales:

1) Crecimiento aditivo/decrecimiento multiplicativo,

2) Arranque lento,

3) Reacción a los eventos de pérdidas.

Crecimiento aditivo/decrecimiento multiplicativo.

Disminuye a la mitad su ventana de congestión cada vez que se produce un evento de pérdida, sin caer por debajo del MSS (máximo tamaño de un segmento).

Una vez que los problemas por la congestión en la red se hayan acabado, la ventana de congestión aumenta (alrededor de 1 MSS de incremento cada tiempo de retardo (RTT del inglés *Round-Trip delay Time* que es el tiempo que tarda un paquete de datos enviado desde un emisor en volver a este mismo emisor habiendo pasado por el receptor de destino.).

Este comportamiento está representado en la Figura 10. Donde al superar el límite de ACK (3 ACK del mismo paquete) la ventana de congestión disminuye, se puede observar a los tres segundos de la Figura 10, causando que la tasa de transmisión disminuya; seguirá decreciendo hasta su límite (1 MSS) o que lleguen ACK de paquetes nuevos, entonces la ventana empieza a incrementar alrededor de 1 MSS en cada RTT

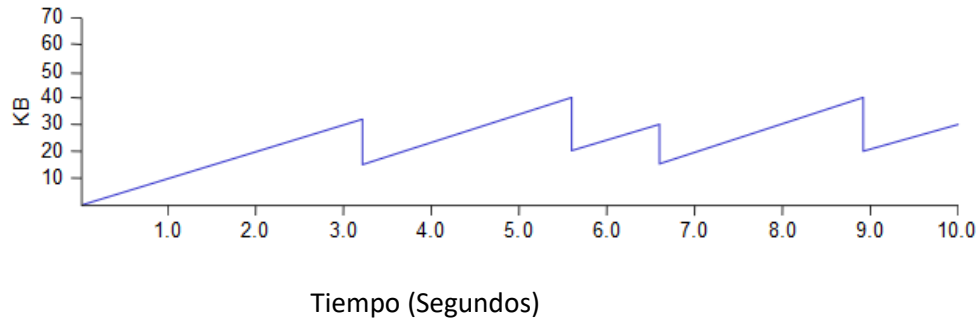


Figura. 10. Esquema del comportamiento diente de Sierra

Arranque lento

Consiste en comenzar enviando un volumen de datos pequeño, que irá aumentando hasta que la red se sature, en cuyo caso se reducirá a la mitad la tasa de envío para reducir la saturación.

2.1.3 Características

Es un protocolo orientado a conexión, Lo que quiere decir es que contro el estado del enlace y asegura que los paquetes lleguen a su destino sin errores. Sus principales características:

- Reordena los paquetes al llegar a su destino.
- Monitorea el flujo de datos y ayuda a evitar la congestión en la red.
- Admite que los datos se agrupen en segmentos de varios tamaños.
- Admite la multiplexación de los datos.
- Comienza y termina la conexión de una manera suave, amablemente.

Confiabilidad de las transferencias

TCP garantiza la transferencia de datos con ayuda del sistema de acuse de recibo que permite al cliente y al servidor garantizar que los datos lleguen sin errores y en el orden correcto.

Al enviar un segmento, se lo vincula a un número de secuencia. Al recibir el segmento y comprobar su estado, el equipo receptor devolverá un segmento de datos con el indicador ACK fijado en 1 acompañado por un número de acuse de recibo que equivale al número de secuencia anterior (Figura 11).

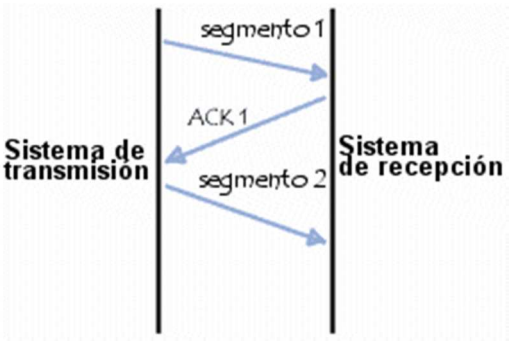


Figura 11 Esquema de transmisión de un segmento TCP

Si el temporizador de retransmisión se ha vencido, sin haber recibido la confirmación de llegada del segmento el equipo considerará al segmento como perdido por lo que, el segmento será reenviado (Figura 12).

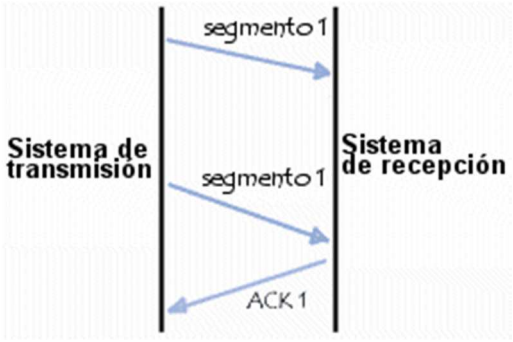


Figura 12 Esquema de retransmisión de un segmento TCP

Si existió algún error y el segmento no se perdió y pudo llegar a su destino, produciendo un segmento duplicado, la máquina receptora sólo retendrá el último segmento que llegó a destino.

2.1.4 Aplicaciones

Muchas aplicaciones y protocolos utilizan TCP para la transmisión de datos debido a su confiabilidad. Las aplicaciones más comunes que usan TCP son:

- **Telnet (*TELecommunication NETwork)*** es un protocolo de Internet estándar que permite conectar terminales y aplicaciones en Internet. Utiliza TCP para la transmisión de datos debido que el protocolo Telnet especifica que los datos deben agruparse de manera predeterminada, esto es si ninguna opción especifica lo contrario, en un búfer antes de enviarse. Específicamente, esto significa que de manera predeterminada los datos se envían línea por línea.

- **Protocolo de Transferencia de Archivos (FTP del inglés *File Transfer Protocol* o)** Es un protocolo para la transferencia de archivos está basado en una arquitectura cliente-servidor. Utiliza a TCP como protocolo de transporte.

- **HTTP (*Hypertext Transfer Protocol* o Protocolo de Transferencia de HiperTexto)** es un sencillo protocolo cliente-servidor que articula los intercambios de información entre los clientes Web y los servidores HTTP.

2.2 Protocolo TCP en medios inalámbricos

2.2.1 Introducción

En teoría, los protocolos de transporte deben ser Independientes de las tecnologías utilizadas en la capa de red. En particular, el TCP no debería preocuparse si el IP está operando por fibra o por radio. En la práctica sí importa, puesto que la mayoría de las implementaciones de TCP han sido optimizadas con base en supuestos que se cumplen en las redes alámbricas, pero no en las inalámbricas. Ignorar las propiedades de la transmisión inalámbrica puede conducir a implementaciones del TCP correctas desde el punto de vista lógico pero con un desempeño horrendo.

Los problemas existentes se basan en la incapacidad de TCP de discriminar cuándo el rendimiento de la conexión ha disminuido debido a pérdidas en el enlace, común en las tecnologías *wireless*, y cuándo es debida a congestión en la red. El problema principal es el algoritmo de control de congestionamiento. Hoy día, casi todas las implementaciones de TCP suponen que las terminaciones de temporización ocurren por congestionamiento, no por paquetes perdidos. En consecuencia, al terminar un temporizador, el TCP disminuye su velocidad y en vía con menor ímpetu.

Desafortunadamente, los enlaces de transmisión inalámbrica son muy poco confiables; pierden paquetes todo el tiempo. El enfoque adecuado para el manejo de paquetes perdidos es enviarlos nuevamente, tan pronto como sea posible. La reducción de la velocidad simplemente empeora las cosas. En efecto, al perderse un paquete en una red alambrada, el transmisor debe reducir la velocidad. Cuando se pierde uno en una red inalámbrica, el transmisor debe acelerar. Cuando el transmisor no sabe de qué clase de red se trata, es difícil tomar la decisión correcta.

Otros aspectos que pueden afectar decisivamente al rendimiento de TCP en una red *Wireless* son: El ancho de banda disponible que en la mayoría de casos es menor que en medios cableados. La posible movilidad de los componentes de la red lo que puede implicar cambios importantes en los tiempos de entrega de los segmentos.

2.2.2 Soluciones Dadas

Definición

Como ya se mencionó el bajo rendimiento de TCP en redes inalámbricas se debe principalmente a la falta de información explícita acerca de lo que causa la pérdida de paquetes en la capa de transporte. Las propuestas para mejorar al TCP actual, en enlaces inalámbricos, debe tener las siguientes características:

- ***End-to-end***: los segmentos solo pueden ser reconocidos al llegar a su destino final.
- ***Local*:** Los cambios deben afectar solo a los nodos que contengan TCP inalámbrico sin afectar el resto de la red.
- ***Two-Way*:** Debe trabajar en dos direcciones tanto desde la red cableada a la inalámbrica como de la inalámbrica a la cableada.

- ***Intermediate-Link***: Debe trabajar sin importar donde se encuentre los nodos inalámbricos dentro de la red.
- ***Transparent*****:** Ningún nodo intermedio necesita saber la información del encabezado TCP.
- ***Signaling*****:** Se comunica con las capas superiores para tomar las medidas adecuadas en la retransmisión.
- ***One-Way***: si está diseñada preferentemente para el tráfico en una dirección.
- ***Last-Hop***: si el algoritmo asume que el enlace *wireless* está ubicado en el extremo final de la conexión TCP.
- ***Snooping***: si se necesita leer en algún nodo intermedio información del encabezado TCP.
- ***Hiding*****:** si presupone que existe un servicio de capa de enlace confiable y que sus protocolos de retransmisión resuelven el problema de la pérdida de tramas, ocultando el carácter *lossy* del enlace, hacia las capas superiores. La principal desventaja de las mejoras que usan esta característica es que, no obstante se oculten las posibles pérdidas, pueden llegar a existir retransmisiones en ambas capas, capa de enlace y de transporte tratando de responder a los mismos eventos de pérdidas, causando interacciones muy indeseables

A continuación se realiza una descripción funcional de algunas de las propuestas existentes que son:

Protocolo *Snoop*

El protocolo *Snoop* es un protocolo de la capa de enlace que interactúa con TCP para mejorar el rendimiento de dicho protocolo en redes inalámbricas. Se basa en la creación de un agente *Snoop* en la estación base que memoriza y compara cada paquete que pasa a través de la conexión TCP en ambas direcciones y mantiene una caché de segmentos

TCP enviados a través del enlace que aún no han sido reconocidas por el receptor, es capaz de determinar, que segmentos se perdieron en el enlace *wireless,* detecta que un paquete se ha perdido con la llegada de reconocimientos duplicados o cuando expira el temporizador local de retransmisiones regido por la llegada de reconocimientos (ACK's) desde el receptor, luego retransmite el paquete perdido y elimina los reconocimiento duplicados. Éste se implementa a nivel de enlace pero tiene en cuenta el funcionamiento del protocolo de transporte de la capa superior (TCP).

Al suprimir reconocimientos duplicados correspondientes a pérdidas en el medio inalámbrico, previene innecesarias invocaciones a métodos de control de congestión.

La principal ventaja de esta propuesta de mejora de la eficiencia de TCP en entornos inalámbricos, es que suprime los reconocimientos duplicados de los segmentos TCP y retransmite localmente los paquetes perdidos de manera que evita que el emisor TCP invoque mecanismos de control de congestión y retransmisión rápida. La Figura 13 muestra el Escenario de aplicación del agente Snoop

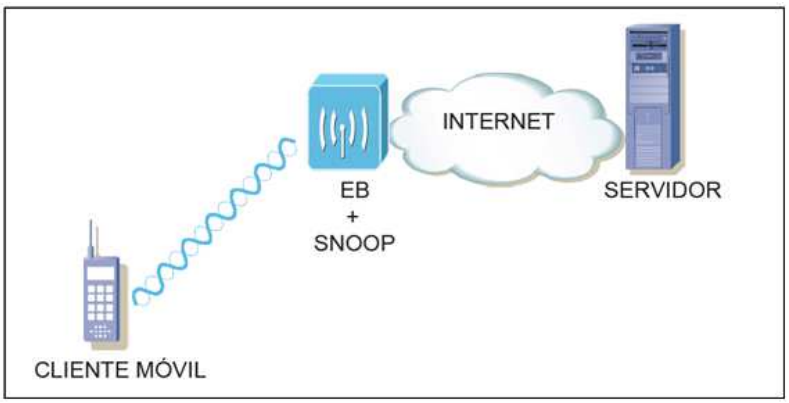


Figura 13 Escenario de aplicación del agente *Snoop*

***Explicit Loss Notification* (ELN)**

Es un mecanismo por el cual se puede comunicar al emisor la razón de la pérdida de los paquetes en especial cuando los errores no estén relacionados con el congestionamiento de la red. Si el receptor o la Estación Base están seguros de que la pérdida de un segmento no es debido a la congestión entonces activa el bit ELN en la cabecera TCP y lo propaga hasta la fuente. Este mensaje del ELN se envía como parte de la misma conexión (y no de manera separada, usando ICMP, por ejemplo).

Esta basado en el protocolo *Snoop* y puede poner remedio a las limitaciones del protocolo *Snoop*. Este protocolo busca mejorar el rendimiento de TCP, cuando la estación móvil es el transmisor TCP. Mediante él, se informa al transmisor TCP que existe una pérdida debida a errores en el enlace inalámbrico, con el fin de evitar la disminución del tamaño de la ventana de transmisión. Por lo que es necesario la instalación de un *Snoop agent* corriendo en la Estación Base, que analiza todos los segmentos TCP que arriban a través del enlace *wireless*. Sin embargo, no los almacena ya que no realiza retransmisión alguna.

Delayed Duplicate Acknowledgments (DDA)

DDA retarda al tercer ACK duplicado, tratando como una pérdida *wireless* y está siendo retransmitido. Si el ACK no llegue luego de determinado tiempo, se libera el ACK duplicado demorado para así comenzar una retransmisión *end-to-end*. Requiere de modificaciones en la estación móvil y no distingue entre pérdida *wireless* y pérdida por congestión.

Explicit Congestion Notification (ECN)

Es una extensión del protocolo de Internet y el Protocolo de control de transmisión y se define en RFC 3168 (2001). ECN permite la notificación de congestión de la red de extremo a extremo sin dejar caer los paquetes. ECN es una característica opcional que sólo se utiliza cuando ambos extremos se apoyan y están dispuestos a usarlo. Sólo es eficaz cuando es apoyado por la red subyacente.

En las actuales redes TCP / IP, TCP depende de la caída de paquetes indicación de congestión. La fuente TCP detecta paquetes perdidos ya sea desde la recepción de tres confirmaciones duplicadas (ACK) o después del tiempo de espera de un temporizador de retransmisión, y responde a un paquete caído al reducir la ventana de congestión.

Convencionalmente, las redes TCP / IP señalan la congestión dejando caer los paquetes. Cuando ECN es negociado con éxito, un router ECN-aware puede establecer una marca en la cabecera IP en lugar de dejar caer un paquete con el fin de la señal de congestión inminente. El receptor del paquete hace eco a la indicación de la congestión para el remitente, lo que reduce su velocidad de transmisión como si se detecta un paquete caído. Algunos equipos de la red anticuados o con errores botan los paquetes que tienen los bits ECN.

"*Explicit Congestion Notification*" esta intrínsecamente unida a la idea de la Administración Activa de Colas (*Active Queue Management* AQM). El objetivo principal de los algoritmos AQM es permitir a los operadores de red lograr un alto rendimiento y bajar la demora promedio al mismo tiempo, por la detención de la congestión inicial. Esto se logra mediante el envío de las indicaciones adecuadas a los puntos finales antes de la cola se desborde. Sin embargo, el método de informar a las fuentes de la congestión no se limita a dejar caer los paquetes, como es el caso de las colas FIFO, donde no se ha habilitado AQM. En cambio, los routers donde se ha habilitado AQM puede marcar los paquetes durante la congestión al establecer el bit ECN en la cabecera de los paquetes, como se había propuesto para el plan de DECbit. El número real y la elección de los paquetes que están marcados durante la congestión dependen de una política AQM particular.

Operación de ECN con IP

ECN utiliza los dos bits menos significativo del campo DiffServ en el IPv4 o IPv6 cabecera para codificar cuatro puntos de código diferentes:

- 00: Non ECN-Capable Transport — Non-ECT
- 10: ECN Capable Transport — ECT(0)
- 01: ECN Capable Transport — ECT(1)
- 11: Congestion Encountered — CE

Cuando los dos extremos soportan ECN, ellos marcan los paquetes con ECT(0) o ECT(1) . Si el paquete atraviesa una cola AQM (por ejemplo, una cola que utiliza *Random Early Detection* (RED)) que está experimentando la congestión y el correspondiente router compatible con ECN, el puede cambiar el punto de código a la CE en lugar de dejar caer el paquete Este acto se conoce como "marca" y su objetivo es informar al extremo receptor de la inminencia de la congestión en el extremo receptor, la indicación de congestión es manejado por el protocolo de capa superior (capa de transporte del protocolo) y las necesita hacer eco de vuelta al nodo de transmisión con el fin de reducir su velocidad de transmisión.

Debido a que la indicación CE sólo pueden ser manejados efectivamente por un protocolo de capa superior que lo soporta, ECN sólo se utilizada en conjunción con los protocolos de nivel superior (por ejemplo, TCP) para:

- Apoyar el control de la congestión,
- Disponer de un método para retornar de la indicación CE al punto final de transmisión.

El funcionamiento de ECN con TCP

TCP soporta ECN con dos banderas en la cabecera TCP. Los dos bits se utilizan para repetir de vuelta la indicación de la congestión (por ejemplo, indicar al emisor que reduzca la cantidad de información que envía) y reconocer que la congestión indicación de eco se recibió. Estos son los segmentos de bits *ECN-Echo* (ECE) y *Congestion Window Reduced* (CWR).

El uso de ECN en una conexión TCP es opcional, para que ECN sea usado, debe ser negociado en el establecimiento de la conexión mediante la inclusión de opciones adecuadas en los segmentos SYN y SYN-ACK.

Cuando ECN se ha negociado en una conexión TCP, el emisor indica que los paquetes IP que llevan los segmentos TCP de conexión que están llevando el tráfico de un transporte capaz de soportar ECN marcándolos con un punto de código ECT. Esto permite que los routers intermedios que soportan ECN marquen los paquetes IP con el punto de código CE en lugar de dejarlos caer con el fin de evitar la congestión de señal.

Al recibir un paquete IP con la congestión experimentados punto de código, el receptor TCP hace eco de esta indicación, la congestión usando la bandera de la CEPE en la cabecera TCP. Cuando un extremo recibe un segmento TCP con el bit de la CEPE se reduce su ventana de congestión como por una caída de paquetes. A continuación, se reconoce la indicación de la congestión mediante el envío de un segmento con el bit CWR.

Un nodo sigue transmitiendo segmentos TCP con el bit ECE hasta que se recibe un segmento con el bit CWR.

ECN y el control de los paquetes TCP

Dado que TCP no realiza control de congestión en los paquetes de control (segmentos ACK puro, SYN, FIN), los paquetes de control no suelen ser marcados como ECN-capable

Una propuesta reciente sugiere marcar los paquetes SYN-ACK como ECN-capable. Esta mejora, conocido como ECN+, se ha demostrado que proporcionan importantes mejoras de rendimiento a las conexiones TCP de corta duración.

Efectos sobre el desempeño

Ya que ECN sólo es eficaz en combinación con las políticas de gestión activa de colas (AQM *Active Queue Management*), los beneficios de la ECN dependen de la AQM precisa que se utilice. Algunas observaciones, sin embargo, parece que se mantienen a través diferentes AQMs.

Como era de esperar, ECN reduce el número de paquetes descartados por una conexión TCP, que, al evitar una retransmisión, reduce la latencia y jitter en especial. Este efecto es más drástico cuando la conexión TCP tiene un segmento de pendiente única, cuando se es capaz de evitar una retransmisión por tiempo de espera, lo que a menudo es el caso de las conexiones interactivas (como inicios de sesión a distancia) y los protocolos de transacciones (por ejemplo, las peticiones HTTP , la fase de conversación de SMTP, o peticiones SQL).

Efectos de la ECN en el rendimiento en transmisiones tipo *bulk* son menos claras, porque las implementaciones modernas de TCP son bastante buenos para volver a enviar segmentos descartados en el momento oportuno, cuando la ventana del emisor es muy grande.

El uso de ECN se ha encontrado ser perjudicial para el rendimiento en redes de gran congestión en el uso de algoritmos AQM que nunca descartar paquetes. Las implementaciones modernas AQM evitar esta trampa dejando caer más que marcar los paquetes con una carga muy alta.

Congestion Coherence (CC)

Asume que esta implementado ECN en la red, usa un esquema basado en la coherencia de la congestión entre paquetes consecutivos apuntando a determinar la causa de la pérdida de los paquetes.

Emplea retransmisiones locales a nivel de capa de Enlace. Los aspectos relevantes de *Congestion Coherence* son:

Retransmisiones locales en capa de Enlace

Todas las tramas trasmitidas en el enlace *wireless* son localmente reconocidas antes de ser borradas en el buffer del emisor. Las tramas que no son reconocidas o son negativamente reconocidas serán retransmitidas cuando el timer expire. Las retransmisiones de las tramas fallidas, tienen mayor prioridad que las nuevas tramas. Con el fin de reducir el retardo de las tramas retransmitidas y minimizar la posibilidad de disparo de retransmisiones *end-to-end* desde el transmisor. Se puede configurar la máxima cantidad de retransmisiones para una trama fallida. La capa de enlace se mantiene retransmitiendo hasta que se alcanza una cantidad máxima de retransmisiones.

Descarte Aleatorio Temprano (RED del inglés Random Early Detection)

Es una gestión activa de colas, evita la congestión mediante el control de tamaño de cola, indicando a los sistemas finales el momento de suspender el envío de los paquetes.

RED es bastante bueno si se desea controlar el tráfico, es mejor que Drop-Tail (Descarte de colas) si se lo utiliza adecuadamente, caso contrario crearía inestabilidad en la red.

2.2.2. Análisis

Snoop

Este protocolo busca descubrir la causa de la pérdida de los segmentos y tomar las acciones que considere pertinentes para prevenir reducciones innecesarias de la ventana de congestión del transmisor TCP.

La principal ventaja de esta propuesta de mejora de la eficiencia de TCP en entornos inalámbricos, es que suprime los reconocimientos duplicados de los segmentos TCP y retransmite localmente los paquetes perdidos de manera que evita que el emisor TCP invoque mecanismos de control de congestión y retransmisión rápida.

Protocolo Snoop es un buen proyecto para mejorar el rendimiento de TCP en la red inalámbrica para comunicar a un *host* fijo a la dirección de un *host* móvil. Pero el protocolo Snoop retransmite el paquete perdido al igual que otras soluciones de la capa de enlace, ahora a nivel local, sino a través de su agente de Snoop. El protocolo Snoop también sufre por no poder proteger por completo el remitente de las pérdidas inalámbrico.

El protocolo S*noop* puede encontrar exactamente la causa de las pérdidas de paquetes y tomar medidas para evitar que TCP efectúe reducciones de ventana innecesarias. Sin embargo tiene algunos problemas como son:

- El protocolo *Snoop* requiere que la estación base mantenga un caché de los segmentos TCP y mantener el estado de conexión, por lo que una carga pesada de procesamiento se suma a la estación base.
- La estación base tiene que comprobar cabecera TCP para encontrar el número de secuencia y el reconocimiento. Cuando los paquetes están protegidos con seguridad IP, esta propuesta no funciona.
- Snooping sólo funciona para el tráfico que va desde el host fijo hacia el host móvil.

Explicit Loss Notification *(ELN)*

Utiliza un bit en la cabecera TCP para comunicar la causa de la pérdida de paquetes al remitente TCP. En la estación base, un agente *Snoop* monitorea todos los segmentos TCP que llegan a través de la conexión inalámbrica, así como *acknowledges* por parte de la red cableada. ELN no almacena en caché los segmentos TCP, pero no pierde de vista los agujeros en el espacio de secuencias TCP. Estos agujeros corresponden a los segmentos que se han perdido por conexión inalámbrica. Cuando un ACK correspondiente a un agujero llega de la red cableada, el bit del ELN en el ACK se fija antes de ser enviado a los datos del remitente. Cuando el emisor recibe un ACK con el bit ELN, retransmite el segmento siguiente, pero no toma ninguna medida de control de congestión. ELN puede detectar la causa exacta de la pérdida de paquetes y tomar las medidas correctas para evitar reducciones innecesarias ventana.

La propuesta del ELN tiene dos propiedades importantes que afectan a la aplicabilidad de las redes inalámbricas.

- Se trata de una propuesta de extremo a extremo: Las modificaciones se realizan únicamente a las capas de protocolo en los dos nodos finales comunicación. Esta propiedad hace que la técnica del ELN escalable y de fácil aplicación en comparación con las propuestas que hay que modificar los nodos de la red interna también.

- Sólo el último eslabón de la conexión (la estación base al nodo móvil) es controlada por la capa MAC del receptor con el fin de detectar pérdidas de paquetes. La comunicación TCP no tienen ninguna información adicional sobre las pérdidas de paquetes en las posibles conexiones inalámbricas internas de la red, ni sobre los paquetes que viajan en dirección de subida. Como consecuencia de ello sólo la dirección de descarga puede ser optimizado por este método.

Por estas razones, la propuesta del ELN es el mejor para aplicar en las redes que sólo contienen enlaces inalámbricos entre los nodos móviles y la estación base. En las redes móviles es muy común tener un solo enlace inalámbrico en el nodo móvil, y la dirección de descarga es todavía dominante en la mayoría de los casos (por ejemplo, navegar por la web), por lo tanto la aplicación de la propuesta del ELN a pesar de estas restricciones puede producir beneficios significativos.

Sus desventajas son:

- Sufre de procesamiento pesado.
- No se puede trabajar con paquetes cifrados.
- Sólo es válida para el tráfico desde el host móvil hacia la estación base
- El ELN introduce retrasos innecesariamente largos para los paquetes retransmitidos.
- Cuando la estación base inalámbrica detecta un error, no pide una retransmisión de inmediato, pero espera ACKs duplicados para volver a activar la retransmisión.

Delayed Duplicate Acknowledgments (DDA)

Algoritmo intenta imitar el comportamiento del protocolo *Snoop*, pero hace modificaciones en el receptor en lugar de la estación base. Cuando se reciben paquetes fuera de orden, el receptor envía ACKs duplicados para los dos primeros paquetes fuera de la orden. Si se pone más de ellos, el receptor difiere ACKs para estos paquetes durante un tiempo *d*. Si durante este período, el siguiente paquete en secuencia llega, el receptor descarta el ACKs duplicados diferidos y envía un nuevo ACK. Si el paquete en secuencia no llega durante este período, el receptor libera el ACKs duplicados diferidos para activar una retransmisión.

DDA es una propuesta sencilla y requiere una modificación sólo en el host móvil. Sin embargo, no puede distinguir inalámbrica y las pérdidas de la congestión, y aumenta la demora por retransmitir paquetes por pérdidas de la congestión.

Explicit Congestion Notification (ECN)

Convencionalmente, las redes TCP / IP señalan la congestión dejando caer los paquetes. Cuando ECN es negociado con éxito, un router ECN-aware puede establecer una marca en la cabecera IP en lugar de dejar caer un paquete con el fin de la señal de congestión inminente.

Explicit Congestion Notification esta intrínsecamente unida a la idea de la Administración Activa de Colas (Active Queue Management AQM). Por lo que el número real y la elección de los paquetes que están marcados durante la congestión dependen de una política AQM particular.

Sus principales desventajas son:

- El receptor del paquete hace eco a la indicación de la congestión para el remitente, lo que reduce su velocidad de transmisión como si se detecta un paquete caído.
- Algunos equipos de la red anticuados o con errores botan los paquetes que tienen los bits ECN
- Aún existen paquetes perdidos debido a la congestión.

Congestion Coherence

Permite configurar la cantidad de intentos al retransmitir mensajes, lo que la vuelve más flexible que otras soluciones; además las retransmisiones fallidas tiene una mayor prioridad que las nuevas tramas, esto se minimiza la posibilidad de un disparo de retransmisiones. .

RED

Es una gestión activa de colas, evita la congestión mediante el control de tamaño de cola, Ayuda con el congestionamiento dentro de la red, si se usa de manera adecuada. Sus principales desventajas son:

- Aumenta el trabajo a los equipos
- Si la configuración no es adecuada, desestabiliza la transmisión de datos
- Su configuración es compleja

CAPÍTULO III
MATERIALES Y MÉTODOS

3.1. Estudio y Selección del software de Simulación

3.1.1 Introducción

Network Simulator (ns)

Es el nombre para una serie de simuladores de redes (ns-1, ns-2 y ns-3), muy fuerte en el estudio de redes, muy flexible ya que nos permite una gran variedad de opciones utilizando un lenguaje de programación dentro de los elementos de simulación.

NS-2

Es un simulador gratuito, más usado en el mundo académico y en los centros de investigación de las principales empresas de IT del mundo, que se suministra con el código fuente completo, nos permite realizar simulaciones de múltiples tipos de redes (cableadas, inalámbricas y por satélite).

Fue desarrollado por el *Information Sciences Institute* de la *University of Southern California*. En dos lenguajes: C++ y OTcl. El C++, para el *core*,. OTcl, para el control. Está diseñado para sistemas operativos Linux, FreeBSD, Solaris, Mac OS X. Puede ser utilizado bajo Windows utilizando Cygwin. Simula un amplio rango de tecnologías de redes como: TCP y UPD, comportamientos de tráfico FTP, Telnet, Web, CBR y VBR, mecanismos de gestión de colas en routers Drop Tail, RED. Soporta diversos algoritmos de enrutamiento (p.e.Dijkstra), implementa multicasting y algunas de las capas de enlace MAC para simular LANs.

No posee una herramienta propia que retorne gráficas de una manera eficiente, sin embargo es fácil conseguir otras herramientas que permiten hacerlo, lo que permite aprovechar el simulador de una mejor manera..

The Enhanced Network Simulator (TeNs)

Es una extensión del simulador Network SImulator que ayuda a solucionar las eficiencias del simulador para modelar el protocolo MAC IEEE 802.11, además incorpora algunas capacidades adicionales como: soporte de múltiples interfaces para nodos móviles, protocolo de ruteo estático para escenarios inalámbricos y para simulación de links a larga distancia.

NS-3

Ns-3 es un simulador de redes de eventos discretos para los sistemas de Internet, dirigidos principalmente para la investigación y el uso educativo. Ns-3 es el software libre, licenciado bajo la licencia GNU GPLv2, y está a disposición del público para la investigación, el desarrollo y uso. NS-3 permite desarrollar simulaciones con un desempeño bastante alto, permitiendo el uso de esta herramienta para simulaciones de redes IP, no IP; así como redes inalámbricas como Wi-Fi, WiMAX, o LTE, además de diferentes protocolos de ruteo entre los que se destacan OLSR y AODV.

Su desventaja es que no se encuentran fácilmente documentación sobre el simulador. El error de muchos es pensar que NS-3 como una actualización de NS-2 ya que NS-3 no es compatible con NS-2 y no se tiene planeado que llegue a serlo.

National Chiao Tung University, Network Simulator (NCTUns)

NCTUns es una poderosa herramienta para simulación y emulación y cuenta con dos características; usa la pila de protocolos TCP/IP o UDP/IP en tiempo real (ral-life) en el kernel (núcleo) de LINUX para realizar simulaciones y emulaciones.

Puede arrancar cualquier programa de aplicación en tiempo real en los nodos de simulación durante la simulación para generar tráfico de red real en las simulaciones. Permite desarrollar, evaluar y diagnosticar el desempeño de protocolos y aplicaciones en diferentes tipos de redes (LAN, MAN, WAN). Las simulaciones hechas con esta herramienta, cuentan con características muy especiales. Estas capacidades hacen que NCTUns genere resultados de simulación de alta con habilidad y proporcione resultados del desempeño de las aplicaciones en tiempo real bajo varios escenarios y condiciones de red.

Se debe tener conocimientos previos en temas de red si se desea manejarlo adecuadamente, ya que sus implementaciones Van enfocadas a comunicaciones en movimiento (e.g., VANETs y MANETs). El simulador necesita de los protocolos TCP/IP de Linux por lo que no puede ser implementado en otro sistema operativo.

OPNET Modeler

Un simulador flexible, es compatible con los sistemas operativos Linux y Windows que permite escalabilidad en modelos jerárquicos. Dichos modelos, están divididos en tres dominios (Red, Nodo y Procesos). Están escritos en C++ y tienen su propio editor.

Es capaz de simular una gran variedad de redes, contando con opciones como flujos de mensajes de datos, paquetes perdidos, mensajes de flujo de control, caída de los enlaces, entre otras. OPNET permite mediante librerías la simulación de nodos con diversas características y la comunicación de los mismos con diferentes tipos de enlaces.

OPNET es un lenguaje de simulación orientado a las comunicaciones, que permite a los programadores acceso directo al código fuente. Este es un simulador utilizado primordialmente por grandes compañías de telecomunicaciones por sus altos costos de licenciamiento.

Cuenta con características que permiten el estudio de los resultados de simulación. en forma de gráficos, presentados dentro de paneles de análisis.

OMNET ++

OMNET++ es una plataforma de simulación de redes, escrita en lenguaje de programación C++. Su arquitectura está formada por un módulo de acceso al medio llamado mac.cc y se encarga de procesar los paquetes y manejar la cola de paquetes por trasmitir.

En comparación con otros simuladores su arquitectura es relativamente sencilla. Todas las simulaciones se componen de objetos C++ llamados SimpleModule que tienen métodos virtuales, privados y protegidos. Sus nodos se componen de una combinación de capas y colas, siguiendo como guía el modelo TCP/IP.

Sus módulos no se encuentras completamente desarrollados lo cual exige al usuario que deba modificarlos o escribir sus propios módulos para cubrir la ausencia de los módulos faltantes dentro del paquete OMNET; esto hace que se necesite un amplio conocimiento no solo sobre redes, también en programación; pues la configuración de módulos no es fácil.

3.2. Parámetros para la selección de una herramienta de simulación

Uso investigativo Aquí calificaremos la cantidad y el tipo de personas que la utilizan y por ende la cantidad de información que exista sobre el simulador.

Alto (5): Muestra que la herramienta es usada tanto por estudiantes cono científicos por lo que existen una gran cantidad de información acerca del simulador como: Manuales, guías, ejemplos, etc.

Medio (3-4): Es usada por la comunidad investigativa. Si bien existe información sobre esta herramienta, está es difícil de conseguir o difícil de entender.

Bajo (1-2): Muy pocas personas lo usan, por lo que su información es escasa o hasta inexistente

Tipo de licencia

Libre (1) Son licencias que los usuarios pueden utilizar, modificar, editar, distribuir, copiar, ejecutar o estudiar el programa de forma gratuita.

Comercial (0) Se llama así cuando necesitas pagar un precio para poder utilizar el programa.

Curva de aprendizaje

Por medio de este parámetro, se busca conocer el grado de conocimiento que el usuario debe tener para poder manejar la herramienta de una manera adecuada.

Alto (5) Es necesario que el usuario posea altos conocimientos sobre redes y acerca del programa para poder manejarlo adecuadamente

Medio (3-4) A este nivel se encuentran las herramientas que se necesita el conocimiento básico acerca de redes y sobre la herramienta

Bajo (1-2) Aquí se encuentran las herramientas de uso didáctico, en las que la configuración de los diferentes elementos se los realiza de manera intuitiva.

Interfaz gráfica

Alto (5) La mayoría de sus elementos y características pueden ser .modificados en una interfaz gráfica, no se necesita conocimiento sobre programación.

Medio. **(3-4)** La interfaz gráfica da un gran apoyo en proyectos básicos; sin embargo, para proyectos de complejidad alta la implementación es necesario realizarlo mediante programación

Bajo (1-2) No posee interfaz gráfica o no es amigable con el usuario, lo cual hace necesario la programación de cada elemento dentro de una simulación para su ejecución final.

Graficación de resultados

Buena (5). Los Simuladores poseen módulos propios para la generación graficas estadísticas que pueden ser manipuladas dentro el mismo simulador y se van actualizando automáticamente

Aceptable (3-4) Simuladores que pueden generar datos estadísticos; sin embargo es necesario de herramientas externas para observarlos con mejor detalle o presentar la información de manera adecuada.

Limitada (1-2) No cuentan con un módulo propio por lo que es necesario sacar la información de otras herramientas externas para poder visualizarlas.

Tráfico que permite modelar

Establece la cantidad y tipo de aplicaciones, servicios o protocolos que la herramienta está en capacidad de simular.

Alto (3) Simulador que tiene una gran variedad de protocolos y características que puede simular

Medio (1-2) Simulador que utiliza varios protocolos; pero no todas sus características.

Nulo (0) Simulador que posee solo los protocolos y características más populares.

Tabla. 8

Comparación de Simuladores

	OPNET	OMNET	NS-2	NS-3	NC-TUNS
Uso investigativo	5	5	5	4	5
Tipo de licencia	0	1	1	1	1
Curva de aprendizaje	5	5	5	5	5
Plataformas que Soporta	Windows / Unix	Windows / Unix	Windows / Unix /MAC	Windows / Unix /MAC	Linux
Interfaz gráfica	5	4	2	4	5
Graficación de Resultados	5	3	2	4	4
Tráfico que permite modelar	3	2	3	2	3

Resolución

Se han analizado los distintos simuladores de redes y se ha decidido usar el simulador NS-2, con la extensión TENS debido a que es un simulador de uso libre, es muy utilizado por lo que existen una gran cantidad de información acerca del simulador.

Se necesita un nivel de conocimientos alto ya que tanto la creación de nodos como sus configuraciones se lo hace a través de un código esto complica la simulación; Sin embargo, una vez conocida la estructura del código se puede hacer grandes cambios solo con la inserción o modificación de una línea de código. Facilitando así la resolución del proyecto.

3.3. Simulaciones

3.3.1 Escenarios

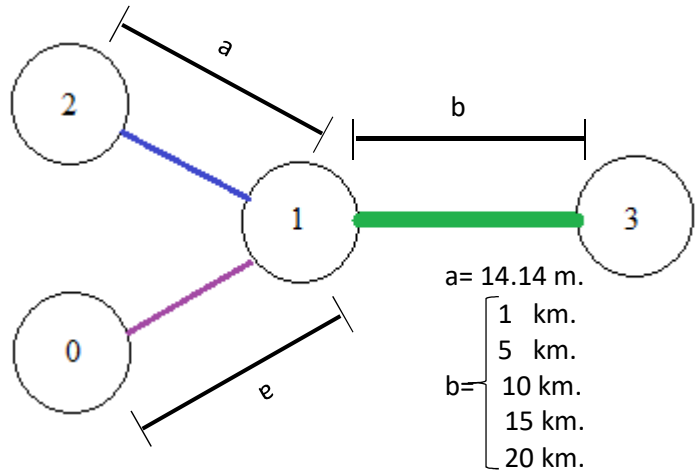


Figura 14 Escenario para simulación

Partiendo del escenario mostrado en la Figura 14 conformado por cuatro nodos inalámbricos con las siguientes características:

- Los nodos cero y dos transmiten simultáneamente, ocasionando congestión, hacia el nodo tres pasando a través del nodo uno.
- Se realizó las simulaciones utilizando primero como protocolo de transporte a TCP sin ningún cambio; luego se realizó las simulaciones con cada una de las soluciones (ECN, TCP 4ACK, RED, RED/ECN, DDA) comparándolos a cada uno con el TCP analizando las mejoras que se producen al utilizar cada una de las soluciones.

El modelo de propagación escogido fue el modelo *FreeSpace* debido a que abarca largas distancias y la simulación no considera interferencias a las diferentes distancias que se toma. La siguiente fórmula representa el umbral del modelo FreeSpace.

$$p_r(d) = \frac{p_t g_t g_r \lambda^2}{(4\pi)^2 d^2 l} \quad (3.1)$$

Donde

p_t = Es la Potencia del nodo transmisor

p_r= Es la Potencia del nodo receptor

g_t= Ganancia del nodo transmisor

g_r= Ganancia del nodo receptor

g_t= Longitud de onda

l = Pérdidas

d = Distancia entre nodos

La Tabla 9 muestra los valores que toman los elementos de la simulación

Tabla. 9

Valores de los datos de la simulación

Elemento	Valor
P_t	0.1 dB
$G_r = G_t$	14 dBi
L	5
Λ	0.125 m
Enrutamiento	Estático

Cada escenario será evaluado en base a la modificación de la distancia entre los nodos 1 y 3, utilizando los valores (1km., 5km., 10km., 15km. y 20 km.). Para cada enlace es necesario calcular la sensibilidad del receptor utilizando la fórmula 3.1 sus resultados se presentarán en la Tabla 10. Por ejemplo se tiene que:

1km.

$P_r(d) = \frac{0.1*14*14*0.125^2}{(4\pi)^2*1000*5} = 3.8787 * 10^{-10}$ dBm.

Tabla 10

Valores necesarios de la sensibilidad de los nodos para cada distancia

Distancia (m)	1000	5000	10000	15000	20000
Sensibilidad	3,8787E-10	1,55148E-11	3,8787E-12	1,72387E-12	9,6968E-13

Escenarios con TCP normal

TCP Se realiza la simulación del comportamiento común del protocolo. Si falla el envío de tres ACK la ventana de transmisión de datos se reduce para evitar la congestión de datos. Para lo cual se utilizará el código descrito a continuación

```
#########################################################
#    CONFIGURACIÓN DE  VARIABLES
#########################################################
```

Se inician las variables como el tipo de canal, el tipo de propagación, el método de enrutamiento, etc.

```
set val(chan)   Channel/Channel_802_11          ;# Tipo de Canal
set val(prop)   Propagation/FreeSpace           ;# Modelo de radio propagación
set val(netif)  Phy/WirelessPhy/Wireless_802_11_Phy  ;# Interface de red
set val(mac)    Mac/802_11                  ; #Tipo de  MAC
set val(ifq)    Queue/DropTail/PriQueue     ; # Tipo de Cola
set val(ll)     LL                          ;
set val(ant)    Antenna/DirAntenna          ; # Antena
set val(ifqlen) 50                          ; # Tamaño de cola
set val(nn)     4                           ; # Cantidad de nodos móviles
```

```
# Variables que determinan el tamaño del campo de simulación

set val(x)      10000000
set val(y)      10000000

set val(rp)     WLSTATIC   ; #Tipo de enrutación (Estática)
set val(ni)     1
set opt(mod)    Modulation/BPSK
set val(erro)   5 ; #Porcentaje de error
 #=========================================================
   # Programa Principal
 #=========================================================
   #
   # Inicia Variables Globales
   #

      set par           [open param.tr w]
      set ns_           [new Simulator]     #Inicio de Variable global simulador

#Creación del archivo que contendrá los datos de los resultados que se analizaran con
TraceGraph
      set tracefd       [open test.tr w]
      $ns_ trace-all $tracefd
      set namtrace      [open test.nam w]
      $ns_ namtrace-all-wireless $namtrace $val(x) $val(y)

   # Creación del área de trabajo

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

```
# Configuración del Nodo con los valores asignadas a las variables anteriormente descritas

        $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) \
                         -channel [new $val(chan)] \
                         -topoInstance $topo \
                         -agentTrace ON \
                         -routerTrace ON \
                         -macTrace ON \
                         -movementTrace OFF \
                         -numif  $val(ni) \


        create-god $val(nn)
```

Aquí se coloca la sensibilidad del receptor RXThresh_, Se recomienda que los valores de RXThresh_, y CSThresh_ sean iguales

```
# Configuración de la capa física
        proc create_node { x y z } {
            global ns_

        #Sensibilidad de los nodos
             Phy/WirelessPhy set RXThresh_ 3.87e-12
            Phy/WirelessPhy set CSThresh_ 3.87e-12
            Mac/802_11 set dataRate_        11mb
            Mac/802_11 set basicRate_       1mb
```

```
        set newnode [$ns_ node]
        $newnode random-motion 0
        $newnode set X_ $x
        $newnode set Y_ $y
        $newnode set Z_ $z
            return $newnode
    }
```

Se crea el protocolo TCP con sus respectivas configuraciones

```
#=============================================
#Configuración del protocolo TCP
#=============================================
proc create_tcp_connection { from to startTime } {
    global ns_ par
    set tcp [new Agent/TCP/Reno] # Selección del tipo de TCP
    $tcp set packetSize_ 1500 #Tamaño del paquete
    $tcp set class_ 2
    set sink [new Agent/TCPSink]  #Creación del agente receptor
    $ns_ attach-agent $from $tcp
    $ns_ attach-agent $to $sink
    $ns_ connect $tcp $sink

    set ftp [new Application/FTP]
    $ftp set packetSize_ 1500
    $ftp attach-agent $tcp
    $ns_ at  $startTime "$ftp start"
    $tcp attach $par
      }
```

Unión del Agente TCP con el agente receptor Sink

Creación de la aplicación FTP con tamaño de paquete de 1500

Unión con el agente TCP

```
#=============================================================
#          Nodo 0
#=============================================================
# Creación y configuración de las características de la antena del nodo


        $ns_ node-config  -numif 1           #Número de interfaces del nodo
        set node_(0) [create_node 10    10      0]     #Ubicación del nodo [X Y Z]
        [$node_(0) set netif_(0)] set channel_number_ 1   # Canal de envío
        [$node_(0) set netif_(0)] set Pt_  0.1 # Potencia de Transmisión
        [$node_(0) set netif_(0)] set L_ $val(erro)  #Porcentaje de erro}

#Configurción de la antena y colocación en el nodo

        set a [new Antenna/DirAntenna]
                        $a setType      1          #Tipo de Antena
                        $a setAngle     45         #Ángulo de ubicación de la antena
                        $a setWidth     10         #Altura de la antena
        [$node_(0) set netif_(0)] dir-antenna $a

#=============================================================
#          Nodo 1
#=============================================================
                $ns_ node-config  -numif 3
                set node_(1) [create_node 20    20      0]
                [$node_(1) set netif_(0)] set Pt_  0.1
                [$node_(1) set netif_(0)] set channel_number_ 1
                [$node_(1) set netif_(0)] set L_ $val(erro)
                set a [new Antenna/DirAntenna]
                        $a setType      1
                        $a setAngle     135
                        $a setWidth     10
                [$node_(1) set netif_(0)] dir-antenna $a


                [$node_(1) set netif_(1)] set Pt_  0.1
                [$node_(1) set netif_(1)] set channel_number_ 6
```

```
        [$node_(1) set netif_(1)] set L_ $val(erro)
        set a [new Antenna/DirAntenna]
                $a setType      1
                $a setAngle     225
                $a setWidth     10
        [$node_(1) set netif_(1)] dir-antenna $a


    [$node_(1) set netif_(2)] set Pt_  0.1
    [$node_(1) set netif_(2)] set channel_number_ 11
    [$node_(1) set netif_(2)] set L_ $val(erro)
    set a [new Antenna/DirAntenna]
            $a setType      1
            $a setAngle     0
            $a setWidth     10
    [$node_(1) set netif_(2)] dir-antenna $a
#=========================================================
#           Nodo 2
#=========================================================
    $ns_ node-config  -numif 1
    set node_(2) [create_node 10    30      0]
    [$node_(2) set netif_(0)] set Pt_  0.1
    [$node_(2) set netif_(0)] set channel_number_ 6
    [$node_(2) set netif_(0)] set L_ $val(erro)
     set a [new Antenna/DirAntenna]
             $a setType      1
            $a setAngle     315
            $a setWidth     10
    [$node_(2) set netif_(0)] dir-antenna $a
```

```
#=========================================================
#          Nodo 3
#=========================================================

        $ns_ node-config  -numif 1

            set node_(3) [create_node 10020  20  0]

        [$node_(3) set netif_(0)] set Pt_  0.1

        [$node_(3) set netif_(0)] set channel_number_ 11
        [$node_(3) set netif_(0)] set L_ $val(erro)
         set a [new Antenna/DirAntenna]
                $a setType      1
                $a setAngle     180
                $a setWidth     10
       [$node_(3) set netif_(0)] dir-antenna $a
#=========================================================
#          Transmisión
#=========================================================

   [$node_(0) set ragent_] addstaticroute 2 1 3 0

   [$node_(2) set ragent_] addstaticroute 2 1 3 0
```

Creación de la ruta de envío de datos
addstaticroute a b c d
a= Número de saltos b= siguiente salto c= nodo receptor d= interfaz de salida

Conexión del protocolo TCP
set tcp0 [create_tcp_connection a b c]
a= nodo emisor b= nodo receptor c= tiempo de inicio de conexión

```
   set tcp0 [create_tcp_connection $node_(0) $node_(3) 1.0 ]

   set tcp1 [create_tcp_connection $node_(2) $node_(3) 1.0 ]
```

```
#=========================================================
#          Finalizar
#=========================================================

   for {set i 0} {$i < $val(nn) } {incr i} {
      $ns_ at 110.0ms "$node_($i) reset";
   }
   $ns_ at 110.0ms "stop"
   $ns_ at 110.01ms "puts \"NS EXITING...\" ; $ns_ halt"
   proc stop {} {
   global ns_ tracefd par
   $ns_ flush-trace
   close $tracefd
   close $par
}
  puts "Starting Simulation..."
   $ns_ run
```

Escenarios con TCP 4 ACK

TCP (4 ACK) A diferencia con el anterior el protocolo TCP espera cuatro ACK para reducir el tamaño de la ventana de transmisión del protocolo. Para lo cual se configura al protocolo TCP para aumentar el número de ACK y esto se lo hace después en la configuración de las características del protocolo.

Para lo cual se utiliza la línea de código en la sección de configuración del protocolo TCP debajo se selección del tipo de TCP

```
$tcp set numdupacks_ #de ack que esperará antes de modificar la ventana
```

Para nuestro caso lo configuraremos en 4 como se muestra a continuación

```
proc create_tcp_connection { from to startTime } {
    global ns_ par
    set tcp [new Agent/TCP/Reno]
        $tcp set numdupacks_ 4
```

Escenarios con RED

RED El protocolo utiliza Detección temprana aleatoria (RED) para reducir la congestión en la transmisión.

Para lo cual modificamos el tipo de cola que acepta el protocolo TCP

```
set val(netif)      Phy/WirelessPhy/Wireless_802_11_Phy
set val(mac)        Mac/802_11              ;
set val(ifq)        Queue/RED
```

Escenarios con ECN

ECN Utiliza la extensión del protocolo IP para disminuir la congestión de red en la transmisión

Se activa la bandera ecn asignando un 1 en la sección de configuración de protocolo TCP

```
proc create_tcp_connection { from to startTime } {
    global ns_ par
    set tcp [new Agent/TCP/Reno]
$tcp set ecn_ 1
```

Escenarios con RED/ECN

RED/ECN Utiliza las dos soluciones anteriores al mismo tiempo por lo que se realizan los cambios efectuados en los dos escenarios anteriores a la vez.

```
set val(ifq)        Queue/RED
$tcp set ecn_ 1
```

Escenarios con Delayed Duplicate Acknowledgments (DDA)

DDA Retarda los ACK duplicados, esperando que la demora sea p-or congestión, con el fin de no disminuir la ventana de transmisión

Se Obtuvo cambiando la línea de código **set** sink [new Agent/TCPSink] por **set** sink [new Agent/TCPSink/DelAck] en la sección de modificación de protocolo TCP dando como resultado:

```
$tcp set packetSize_ 1500
$tcp set class_ 2
set sink [new Agent/TCPSink/DelAck]
$ns_ attach-agent $from $tcp
```

CAPÍTULO IV
ANÁLISIS DE RESULTADOS Y FORMULACIÓN DE LA SOLUCIÓN

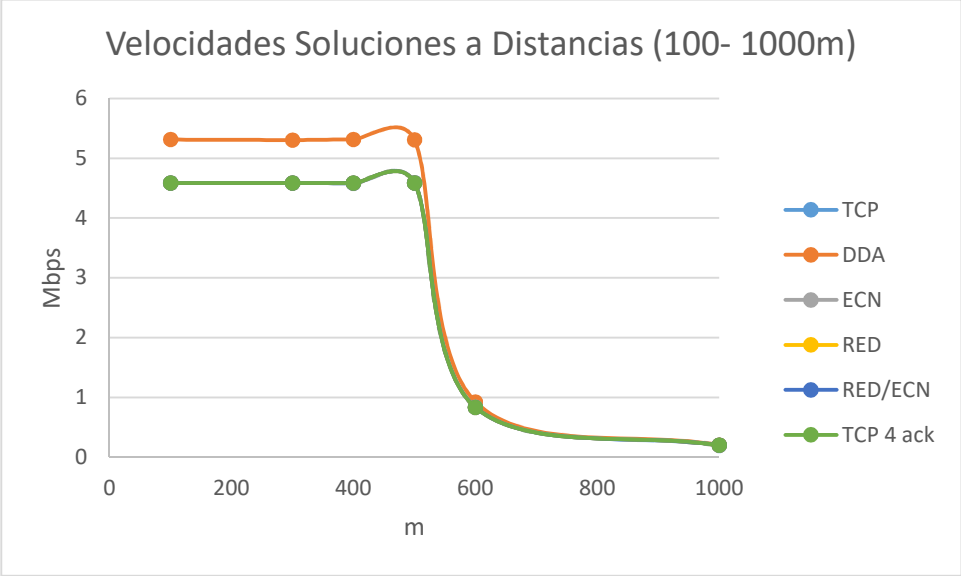


Figura 15 Velocidad a diferentes distancias TCP

La Figura 15 nos muestra el comportamiento de la velocidad que toman las soluciones a distancias menores de 1km. Para la transmisión se utiliza el estándar 802.11 b que tiene una velocidad teórica de 11 Mbps; Sin embargo, "Debido al espacio ocupado por la codificación del protocolo CSMA/CA, en la práctica, la velocidad máxima de transmisión con este estándar es de aproximadamente 5.9 Mbit/s sobre TCP y 7.1 Mbit/s sobre UDP". Si añadimos a esto la congestión causada por el envió simultaneo de dos nodos obtenemos la velocidad mostrada en la Figura 16. Como se puede ver la única solución que mejora la transmisión en distancias menores a un kilómetro es DDA.

4.1. Análisis de Resultados

Como se puede observar en la Figura 15, debido al cambio brusco de velocidades entre la velocidad a distancias recomendadas para el uso del WiFi y las velocidades de Wild, no es posible ver de manera clara las diferencias entre las velocidades de las soluciones, por lo que se analizará las velocidades en distancias mayores de 1km. Para lo cual se escogió hacer un promedio de tres simulaciones debido a que no existía una diferencia significativa entre cada simulación.

4.1.1 Comparación del Throughput de paquetes recibidos

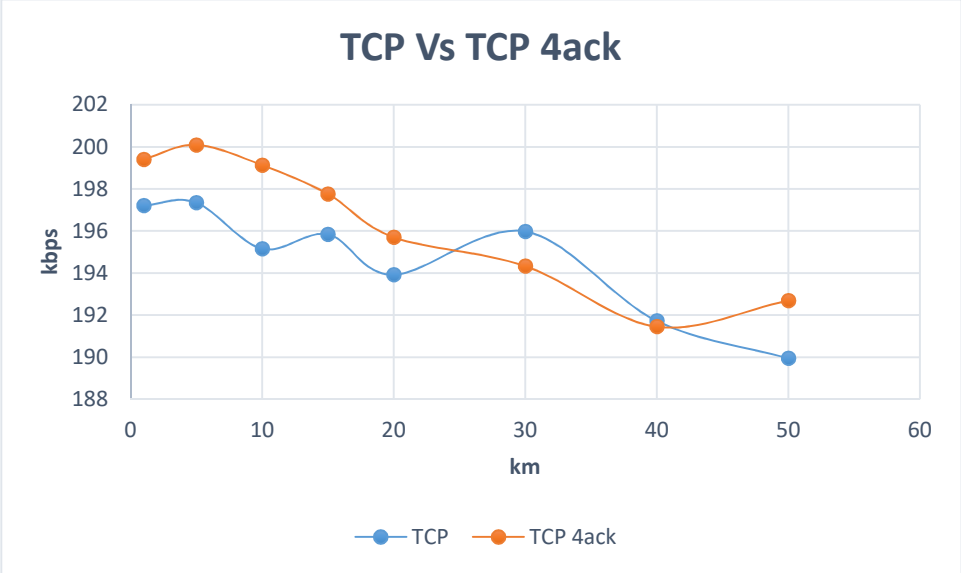


Figura 16 Promedio de velocidad a varias distancias TCP & TCP (4ACK)

La Figura 16 nos muestra las distintas velocidades entre estas dos soluciones. Se puede apreciar que la diferencia de velocidades no es mucha, aun así la velocidades de TCP (4ACK) es más estable y hasta los 20 km. supera la velocidad de TCP normal.

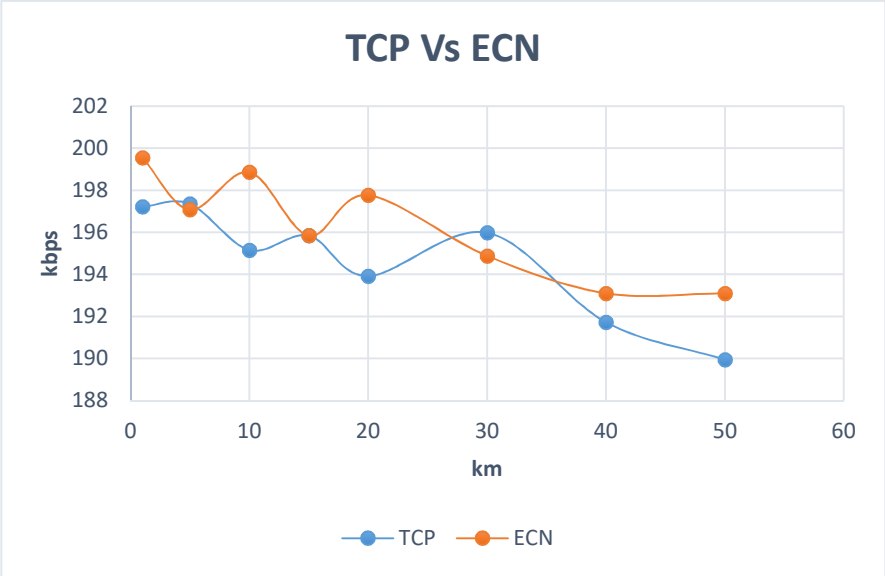


Figura 17 Velocidad a diferentes distancias TCP & ECN

La Figura 17 nos muestra las diferencias en cuanto a la velocidad entre estas dos soluciones. Se puede apreciar que la diferencia de velocidades no es mucha. Aún así ECN supera en velocidad a TCP normal.

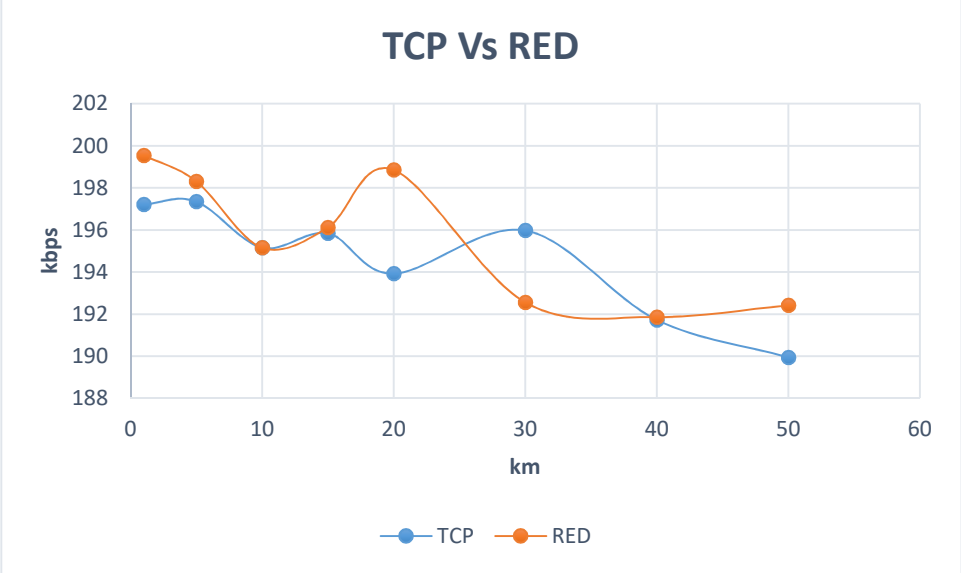


Figura 18 Velocidad a diferentes distancias TCP &RED

La Figura 18 nos muestra las distintas velocidades entre estas dos soluciones. La diferencia de velocidades es mínima y hasta más baja que la

del TCP normal, debido a todo el procesamiento que debe realizar antes enviar un paquete,

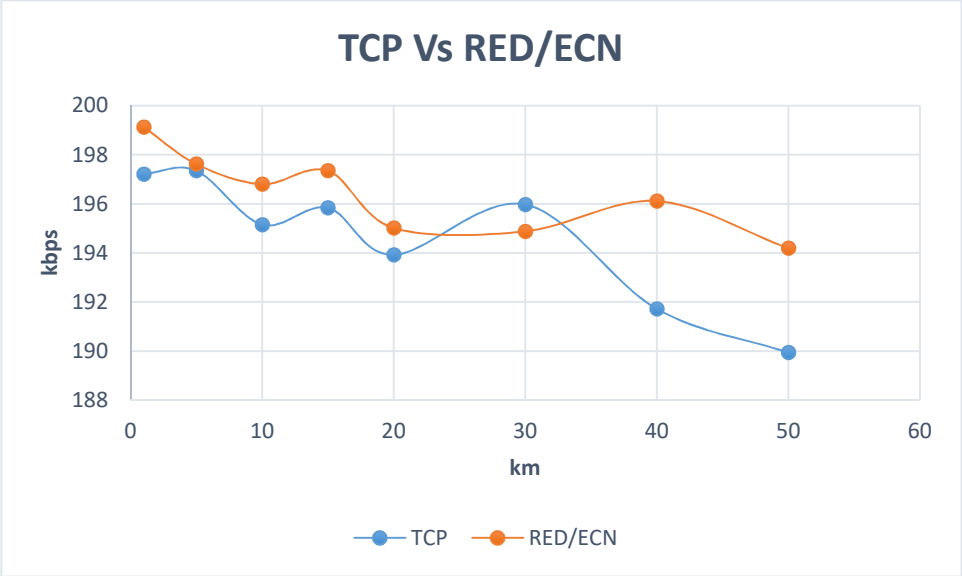


Figura 19 Velocidad a diferentes distancias TCP &RED/ECN

La Figura 19 nos muestra las distintas velocidades entre estas dos soluciones. La velocidad de la solución RED/ECN es bastante estable y mayor que la del TCP normal.

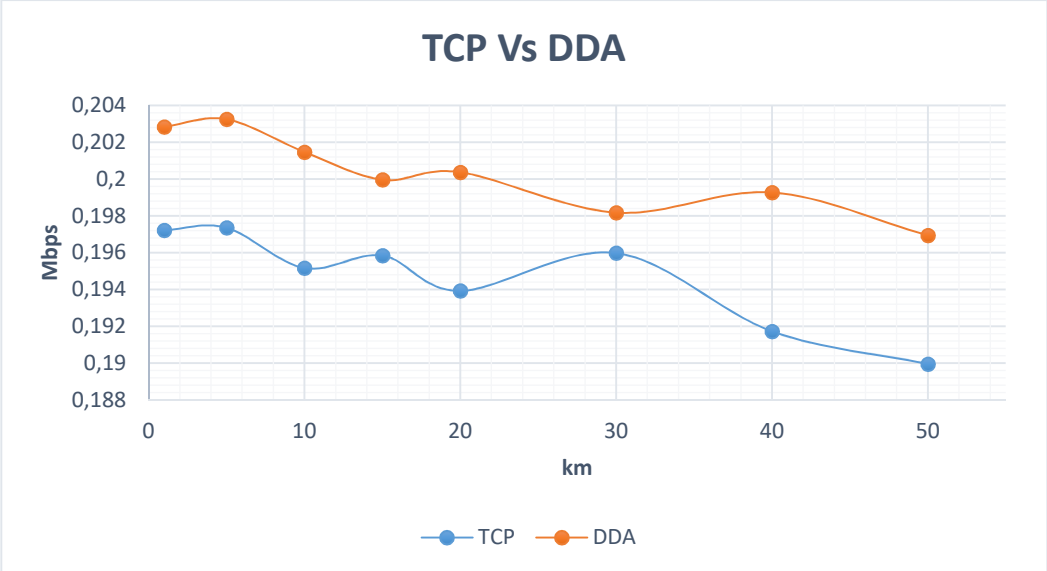


Figura 20 Velocidad a diferentes distancias TCP & DDA

La Figura 20 nos muestra las distintas velocidades entre estas dos soluciones. Es la solución que mantiene la mayor velocidad entre todas, además es muy estable.

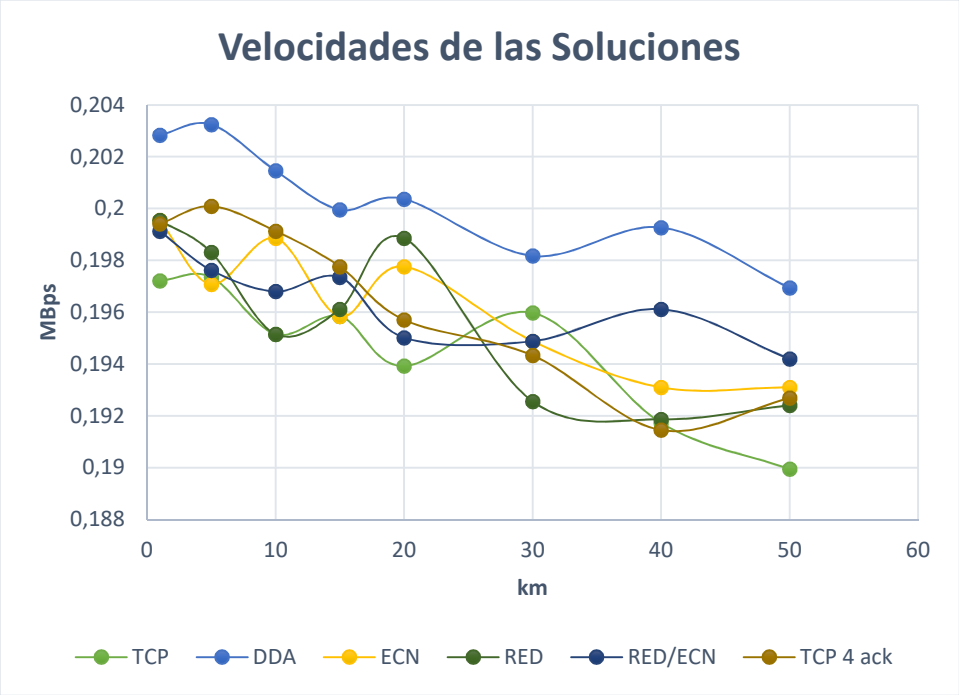


Figura 21 Velocidad a diferentes distancias de las soluciones

Análisis

Para determinar la solución que posee la mayor velocidad utilizamos el área debajo de las curvas de cada una de las velocidades. Como se lo puede observar el la Figura 21 se puede observar que la solución DDA sobrepasa a las demás en todas las distancias. Tomándola como referencia tenemos la relación que existe las otras velocidades en relación a esta como se aprecia en la Figura 22.

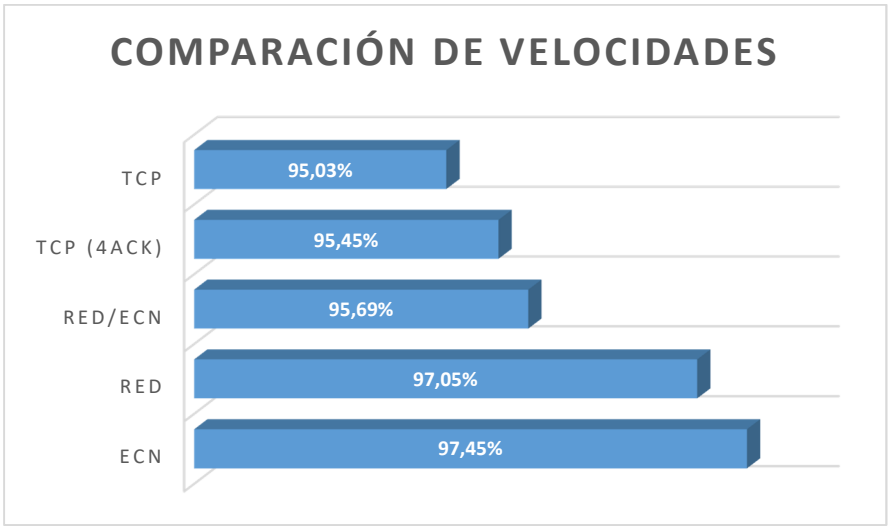


Figura 22: Relación de las velocidades de las soluciones con DDA

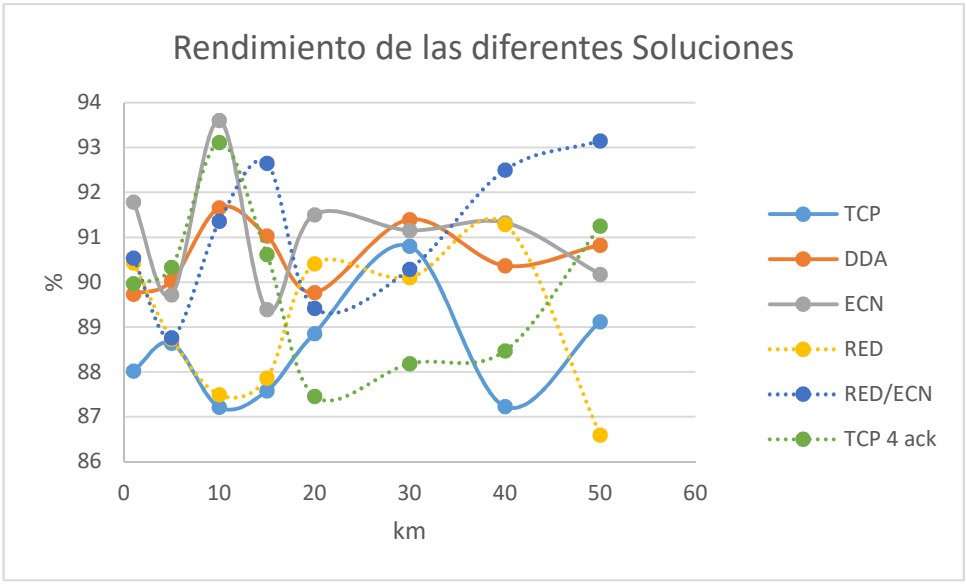


Figura 23 Rendimiento a diferentes distancias Todas las soluciones

Para encontrar el rendimiento de las diferentes soluciones se obtiene a través de la siguiente fórmula:

$$\eta = \frac{bits\ enviados}{bits\ recibidos} \quad (4.1)$$

Los bits enviados son tomados de los nodos emisores (nodo 0 y nodo 2). Los bits recibidos se los toma del nodo receptor (nodo 3)

La Figura 23 muestra el rendimiento de las distintas soluciones, tomando la relación de los bits que llegaron con los bits enviados. Viendo la Figura 22 vemos que tanto la solución RED como TCP (4ACK) su rendimiento decae por debajo de TCP normal por lo que solo nos fijaremos en DDA y ECN las cuales superan el rendimiento de TCP normal en cada una de las distancias simuladas.

Al igual que las velocidades se tomarán en cuenta el área de la curva obteniendo que la mayor área es de la solución ECN por lo que en comparación con esta tenemos lo mostrado en la Figura 24.

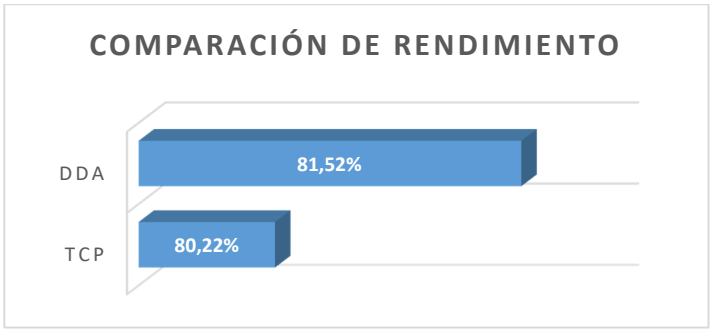


Figura 24: Relación del rendimiento de las soluciones con ECN

4.1.2 Comparación entre el valor promedio del retardo de cada solución

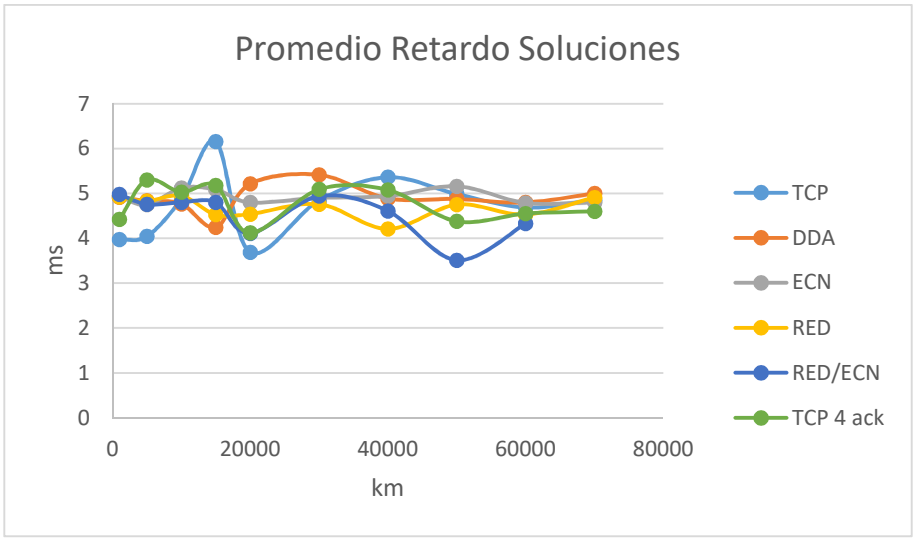
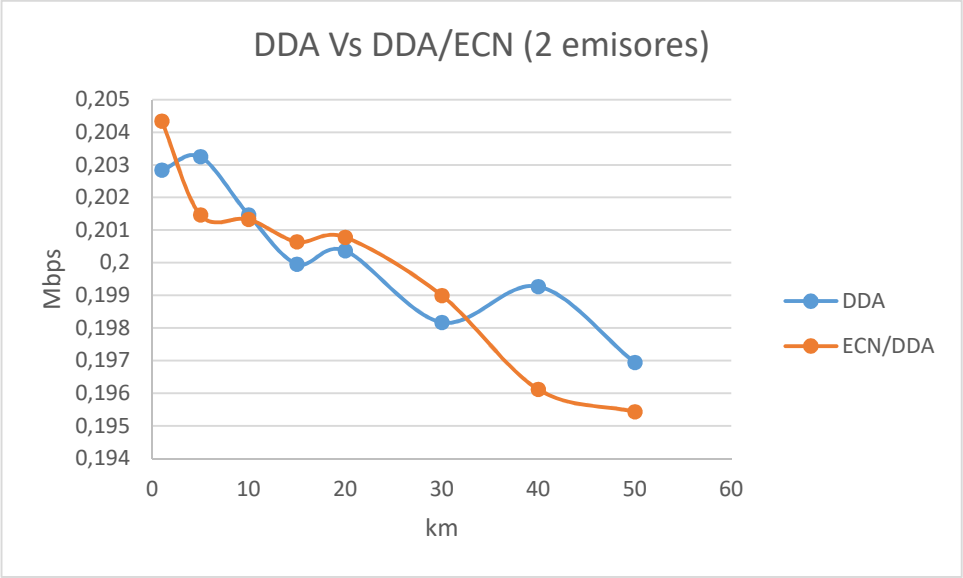
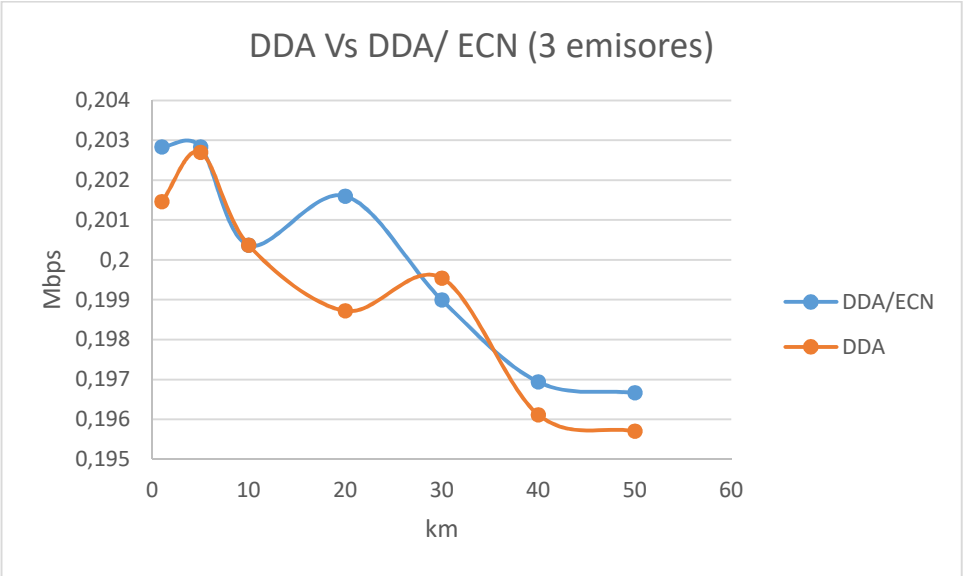


Figura 25 Retardo promedio retardo de paquetes.

La Figura 25 nos muestra el retardo promedio que tiene en la transmisión las dos soluciones a distintas distancias. Como se puede apreciar la diferencia entre los retardos entre cada solución con el TCP normal es mínima por lo que no se tomará en cuenta para decidir la mejor solución.



(a)



(b)

Figura 26 Velocidad a diferentes distancias DDA & DDA/ECN (a) 2 nodos emisores (b) 3 nodos emisores

La Figura 26 nos muestra que la solución DDA/ECN mantiene la misma velocidad que DDA y mientras los emisores van aumentando y por lo tanto el tráfico la solución DDA/ECN no decae su velocidad y empieza a sobrepasar levemente a la solución DDA.

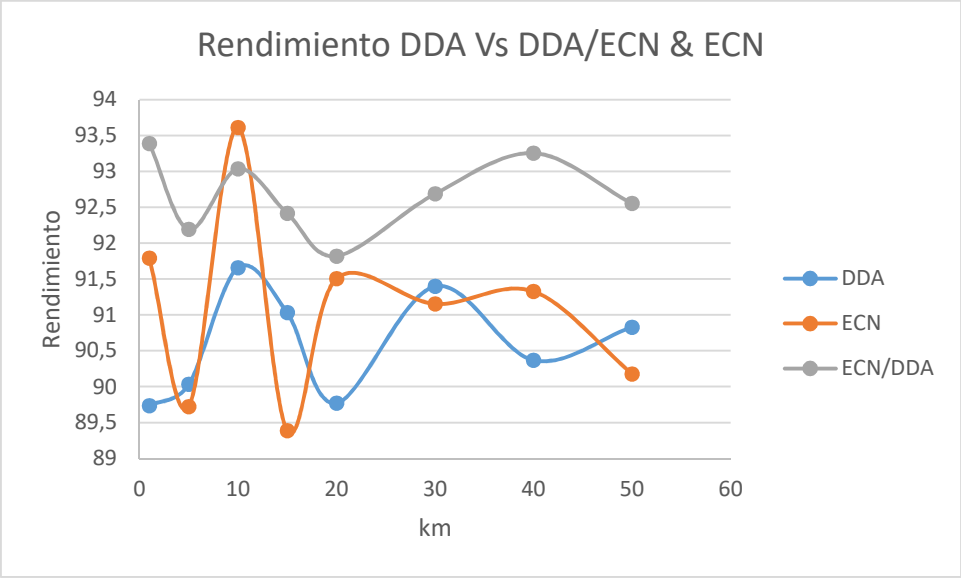


Figura 27 Comparación del rendimiento de las soluciones ECN, DDA & DDA/ECN

La Figura 27 nos muestra el rendimiento que tienen las tres soluciones y se puede apreciar que la solución DDA/ECN tiene un mejor rendimiento que las otras dos soluciones

CAPÍTULO V
CONCLUSIONES Y TRABAJOS FUTUROS

En el presente trabajo se analizaron a varias alternativas que solucionaban de alguna medida el problema de TCP en medios inalámbricos, comparando su comportamiento, velocidad, jitter en ambientes de larga distancia para determinar las condiciones para el mejor funcionamiento de cada una de las soluciones.

A continuación se describirán las conclusiones del presente trabajo y algunos de los posibles trabajos futuros que pueden continuar desarrollándose como resultado de la investigación.

5.1 Conclusiones

Se encontraron varias soluciones: TCP (4ACK), RED, ECN, DDA, RED/ECN. Se encontró que si bien todas las soluciones mejoran el rendimiento del TCP inalámbrico en ambientes de larga distancia, su velocidad es diferente entre ellas. Las soluciones ECN y DDA son aptas en ambientes de largas distancias, pues mantienen una velocidad mayor y estable que las otras soluciones. Las soluciones TCP 4ACK y RED no son aptas debido a que la diferencia de velocidad con el TCP normal no es estable.

Para simular el comportamiento en largas distancias se necesita modificar el valor de Slot Time ya que son los encargados de medir el tiempo en que el receptor espera el mensaje del emisor antes de asignarlo como paquete perdido; para lo cual se utiliza el complemento TENS para el simulador NS-2 que automáticamente cambia los temporizadores (*Slot Time)* de un valor constante a trabajar en función a los *Air Propagation Time (*Temporizador de Propagación por Aire) lo que permite que el usuario solo deba colocar la

distancia a simular. Se debe colocar la sensibilidad del receptor, con el comando *Phy/WirelessPhy set RXThresh_ valor de la sensibilidad.* Para encontrar el valor que debe tener la sensibilidad se puede utilizar las opciones que vienen dentro del simulador o manualmente con fórmulas sobre propagación, expuestas en capítulos anteriores.

Después de haber simulado las distintas soluciones diversas distancias, se puede reconocer que el DDA tuvo un mejor comportamiento que las otras respuestas. Comparándola con las otras respuestas tenemos que: la diferencia en el retardo y el rendimiento es despreciable, su velocidad es la mayor de las otras soluciones, su velocidad es mejor en casi 2.55 % con ECN. y con 5% del TCP normal. Si bien no posee un método para controlar el congestionamiento en la red; esto no es muy importante ya que WILD suele utilizarse en su mayoría para realizar conexiones en localidades lejanas donde la congestión no es el principal problema. En los pocos casos donde sea indispensable disminuir el problema de la congestión y se posea elementos que soporten la carga de trabajo se puede utilizar los métodos de RED, ECN y RED/ECN que si bien no poseen una mejora significativa en cuanto a la velocidad, mejora la estabilidad del Throughput y disminuyen la cantidad de paquetes caídos.

La mejor solución sería trabajar de manera híbrida DDA y ECN. DDA es la solución con mejor velocidad; sin embargo, no posee una manera de ayudar con la congestión en la red, lo que puede ser compensado usando ECN. Las dos soluciones no ejercen una gran cantidad de carga a los equipos con los que se trabajan, ni se requiere un gran conocimiento para configurar los equipos. Como se puede apreciar en las Figuras 26 y 27 mantiene la velocidad de la solución DDA pero mejora su rendimiento alrededor de 2% en comparación con DDA y ECN.

5.2 Trabajos Futuros

Como continuación de este trabajo de investigación, el grupo de trabajo está interesado en comprobar los resultados en ambientes reales. Además se desea analizar otras soluciones que no fueron posible de simular como: TCP NACK; el cual utiliza banderas que indican si el problema es causado por congestión o por pérdidas en el medio, además disminuye la cabeza de TCP, ELN y Snoop. Soluciones que verifican si un ACK es causado por congestión o si se perdió en el medio de transmisión.

REFERENCIAS BIBLIOGRÁFICAS

(s.f.). Obtenido de http://ieeestandards.galeon.com/aficiones1573579.html

Avilés. (s.f.). *Óptica Reflexión Y Refracción*. Obtenido de http://web.educastur.princast.es/proyectos/fisquiweb/Apuntes/Apuntes2Fis/ReflexionRefraccion.pdf

Buchholcz, G. G. (s.f.). *Explicit Loss Notification to Improve TCP Performance over Wireless Networks .*

Ermanno, P. (2007). *Unidad 17: Enlaces de Larga Distancia.* Obtenido de http://www.itrainonline.org/itrainonline/mmtk/wireless_es/files/17_es_enlaces-larga-distancia_guia_v03.pdf

Floyd, S. (s.f.). *TCP and Explicit Congestion Notification, Lawrence Berkeley Laboratory.*

García Bauza, C., Vénere, M., Parente, L., & Lotito, P. (2009). *RED, ALGORITMO DE CONTROL DE CONGESTION EN REDES IP*. Obtenido de http://www.cimec.org.ar/ojs/index.php/mc/article/viewFile/2906/2843

Grupo de Telecomunicaciones Rurales. (2009). *WiLD WiFi Based Long Distance.* Lima-Perú.

Historia del protocolo TCP/IP. (s.f.). Obtenido de https://sinfallas.wordpress.com/2015/02/03/historia-del-protocolo-tcpip/

Kioskea.net. (Junio de 2014). *Introducción a Wi-Fi (802.11 o WiFi)*. Obtenido de http://es.ccm.net/contents/789-introduccion-a-wi-fi-802-11-o-wifi

KNOTIK. (s.f.). *Aplicaciones Wireless.*

Las características del protocolo TCP. (s.f.). Obtenido de http://es.ccm.net/contents/281-protocolo-tcp

Maracara, M. (s.f.). *Simulación de teletrafico*. Obtenido de http://simuladorns2.blogspot.com/

RFC 793. (1981). *Transmision Control Protocol".IETF*. Obtenido de http://tools.ietf.org/html/rfc793

Rodríguez, F., Vidal, L., & Alves, L. (s.f.). *TCP sobre enlaces Wireless Problemas y algunas posibles soluciones existentes*. Obtenido de https://www.researchgate.net/publication/237236848_TCP_sobre_enlaces_wireless_Problemas_y_algunas_posibles_soluciones_existentes

Shie-Yuan Wang & Yi-Bing Lin. (2005). *NCTUns network simulation and emulation for wireless resource management.*

Suarez, A. (2009). *Sistemas de Conmutación: Control de congestión*. Obtenido de http://es.slideshare.net/And3es/sistemas-de-conmutacin-control-de-congestin

Varma, V. K. (2006). *Wireless Fidelity - WiFi.*

Wireless QoS. (2010). Obtenido de http://www.revolutionwifi.net/revolutionwifi/2010/07/wireless-qos-part-1-background_7048.html