



Características estadísticas de la topología  
de las redes ad hoc móviles y evaluación de  
estrategias para mantener redes lógicas

Tesis que presenta  
Adán Geovanni Medrano Chávez  
para obtener el grado de  
Doctor en Ciencias y Tecnologías de la Información

Asesores: Dra. Elizabeth Pérez Cortés y Dr. Miguel López Guerrero

Jurado calificador:

Presidente	Dr. Rolando Menchaca Méndez	CIC
Secretario	Dr. Víctor Manuel Ramos Ramos	UAM-I
Vocal	Dr. Víctor Rangel Licca	UNAM
Vocal	Dr. Ricardo Marcelín Jiménez	UAM-I
Vocal	Dr. Michael Pascoe Chalke	UAM-I

Ciudad de México, marzo de 2016



Características estadísticas de la topología  
de las redes ad hoc móviles y evaluación de  
estrategias para mantener redes lógicas

Tesis que presenta  
Adán Geovanni Medrano Chávez  
para obtener el grado de  
Doctor en Ciencias y Tecnologías de la Información

Asesores: Dra. Elizabeth Pérez Cortés y Dr. Miguel López Guerrero

Jurado calificador:

Presidente	Dr. Rolando Menchaca Méndez	CIC	_____
Secretario	Dr. Víctor Manuel Ramos Ramos	UAM-I	_____
Vocal	Dr. Víctor Rangel Licea	UNAM	_____
Vocal	Dr. Ricardo Marcelín Jiménez	UAM-I	_____
Vocal	Dr. Michael Pascoe Chalke	UAM-I	_____

Ciudad de México, marzo de 2016

# Resumen

Actualmente, los dispositivos móviles podrían formar redes que permitan que sus usuarios compartan y hagan uso de los recursos de otros sin usar la infraestructura de comunicaciones convencional. Para este fin, las terminales de usuario pueden interconectarse de manera autoorganizada y descentralizada para formar una infraestructura volátil conocida como red ad hoc móvil. Además, se debe formar una red par a par sobre esa infraestructura para ofrecer un servicio de búsqueda encargado de descubrir la identidad de los proveedores de recursos compartidos. Las redes par a par operan exitosamente sobre infraestructuras de comunicación como la Internet. No obstante, formarlas sobre una red ad hoc móvil es un reto de interés ya que la infraestructura presenta dos características que, en general, dificultan la ejecución de aplicaciones distribuidas: un caudal de datos limitado y una topología física dinámica. Para hacer frente a estos retos es necesario que los servicios provistos por las redes par a par sean eficientes y se ajusten a las características de las redes ad hoc móviles. No obstante, este tipo de servicios aún no integra mecanismos y estrategias para operar eficientemente en redes ad hoc móviles. Esta aseveración se fundamenta en que, en su mayoría, las soluciones actuales se construyeron sin considerar que son humanos los que portan los dispositivos que conformarían la red. Además, dichas soluciones no consideran los mecanismos que hacen que los servicios de búsqueda se ejecuten exitosamente en redes par a par formadas sobre la Internet. En consecuencia, no es posible asegurar que las propuestas presentadas hasta ahora operen eficientemente en redes ad hoc móviles integradas por terminales portadas por humanos. Partiendo de estos hechos, la presente tesis doctoral se centra en determinar tanto los mecanismos citados como el efecto de la movilidad humana en la topología de una red ad hoc móvil y en protocolos ejecutados sobre ésta. Para desarrollar dicho conocimiento se realiza un extenso análisis por simulación de eventos discretos cuyo resultado determina: (1) los mecanismos que vuelven confiables a las tablas *hash* distribuidas en redes lógicas con topología dinámica, (2) las características estadísticas que las redes ad hoc móviles exhiben cuando el movimiento de los nodos corresponde a las propiedades de la movilidad humana y (3) las estrategias estabilizantes que hacen que las redes lógicas de tipo jerárquico mantengan su formación tanto como sea posible. Este conocimiento constituye una base que permite prestar servicios eficientes de búsqueda par a par en redes ad hoc móviles.

Con todo el corazón a quien camina conmigo los senderos de la vida  
Zelzin Marcela Márquez Navarrete

# Reconocimientos

Esta tesis doctoral es fruto del esfuerzo de cuatro años de constante dedicación y empeño. No hubiera sido posible finalizarla sin la guía de mis estimados asesores, a quienes agradezco el valioso tiempo que invirtieron durante el desarrollo de este proyecto. Además, agradezco a los miembros del jurado calificador por los consejos que dieron para mejorar la calidad de este escrito. Finalmente, agradezco al CONACyT por la beca que me otorgó.



# Índice general

<b>1. Introducción</b>	<b>1</b>
1.1. Problema de investigación . . . . .	6
1.2. Objetivo general . . . . .	6
1.3. Objetivos particulares . . . . .	6
1.4. Metodología general . . . . .	7
1.5. Lista de contribuciones . . . . .	8
1.6. Estructura de la tesis . . . . .	9
<b>2. Lecciones aprendidas de redes P2P estructuradas con infraestructura</b>	<b>11</b>
2.1. Tablas hash distribuidas . . . . .	13
2.1.1. Chord . . . . .	14
2.1.2. Kademlia . . . . .	16
2.2. Marco de evaluación . . . . .	19
2.2.1. Modelado de la rotación de los participantes . . . . .	20
2.2.2. Medidas de desempeño . . . . .	21
2.2.3. Metodología experimental . . . . .	23
2.3. Resultados . . . . .	27
2.3.1. Evaluación en condiciones de cambio abruptas . . . . .	27
2.3.2. Evaluación con pares estables . . . . .	30
2.4. Discusión . . . . .	31

<b>3. Análisis experimental de características topológicas de las MANET</b>	<b>35</b>
3.1. Revisión de la literatura . . . . .	36
3.1.1. Modelos de movilidad . . . . .	37
3.1.2. Protocolo de encaminamiento AODV . . . . .	40
3.1.3. Trabajo relacionado . . . . .	43
3.2. Metodología experimental . . . . .	44
3.2.1. Medidas de desempeño . . . . .	45
3.2.2. Configuración de la simulación . . . . .	47
3.3. Resultados . . . . .	50
3.3.1. Análisis de la topología de red . . . . .	50
3.3.2. Desempeño de AODV . . . . .	55
3.4. Discusión . . . . .	60
<b>4. Análisis de estrategias estabilizantes para redes jerárquicas</b>	<b>63</b>
4.1. Estrategias estabilizantes . . . . .	68
4.1.1. Estrategias basadas en criterios de elección de líder . . . . .	68
4.1.2. Estrategias basadas en políticas de validez relajadas . . . . .	70
4.1.3. Políticas de reorganización local . . . . .	71
4.2. Marco de evaluación . . . . .	72
4.2.1. Estrategias de estabilización evaluadas . . . . .	72
4.2.2. Algoritmo de agrupamiento . . . . .	75
4.2.3. Medidas de evaluación . . . . .	77
4.2.4. Configuración de las simulaciones . . . . .	79
4.3. Resultados . . . . .	80
4.3.1. Características estadísticas de la red jerárquica . . . . .	80
4.3.2. Estabilidad de la red jerárquica . . . . .	83



4.3.3. Costo del mantenimiento de la red jerárquica . . . . .	87
4.4. Discusión . . . . .	90
<b>5. Conclusiones y perspectivas</b>	<b>93</b>
5.1. Bases para el diseño de un servicio de búsqueda P2P eficiente . . . . .	94
5.2. Líneas de investigación . . . . .	96



# Índice de tablas

2.1. Configuración de las tablas <i>hash</i> distribuidas. . . . .	24
2.2. Composición de red P2P heterogénea. Notación: $\overline{T_{on}}$ es el tiempo en línea medio; $C_n$ significa composición número $n$ . . . . .	27



# Índice de figuras

2.1. Espacio de claves y tabla de atajos del nodo 146. . . . .	14
2.2. Espacio de claves de Kademlia con longitud $m = 4$ bits y contenedores de longitud $k = 1$ del nodo 0011. . . . .	17
2.3. Representación gráfica de la rotación de los participantes. . . . .	25
2.4. Desempeño mostrado por las tablas <i>hash</i> distribuidas Chord y Kademlia en (a) términos de confiabilidad y (b) costo de mantenimiento. . . . .	28
2.5. Desempeño mostrado por Chord y Kademlia evaluados en una red con distintas composiciones de participantes. (a) Nivel de confiabilidad. (b) Costo de mantenimiento. . . . .	30
3.1. Muestras de un viaje recorrido por un nodo bajo (a) el modelo SLAW y (b) el modelo RWP. . . . .	49
3.2. Razón de conectividad mostrada por los modelos de movilidad RWP y SLAW en redes de (a) 25, (b) 100 y (c) 300 nodos. En (d) se muestra la razón de aislamiento. . . . .	52
3.3. Número promedio de vecinos por salto en redes de (a) 25, (b) 100 y (c) 300 nodos. (d) Vecinos del nodo 299 hasta seis saltos en un escenario de red configurado con RWP y tamaño de red igual a 300 nodos. . . . .	54
3.4. Razón de búsquedas exitosas medida en redes de (a) 25, (b) 100, (c) 300 nodos. . . . .	56
3.5. RTT medido en redes de (a) 25, (b) 100, (c) 300 nodos. . . . .	57
3.6. Tiempo de vida de las rutas creadas por el protocolo AODV medido en redes de (a) 25, (b) 300 nodos. . . . .	59

4.1.	(a) Red inválida bajo la política estricta, pero válida bajo la política flexible. (b) Red lógica mostrada en la figura (a) corregida empleando la política de delegación de rol con $k = 2$ y $d = 1$ . . . . .	74
4.2.	Resultados que describen las características estadísticas de los grupos bajo el modelo de movilidad SLAW. (a) Tamaño promedio. (b) CCDF del tamaño de los grupos. (c) Números promedio de grupos. (d) Red jerárquica de 300 nodos formada bajo la configuración $(k_2, \neg i, d_0)$ . . . . .	81
4.3.	Nivel de estabilidad provisto por distintos criterios de elección de cabezas de grupo. (a) CCDF del tiempo de vida de grupo ( $T_{\text{cluster}}$ ). (b) Razón de desintegración $D_r$ debida a invalidaciones y aislamiento de cabezas de grupo. . . . .	83
4.4.	Nivel de estabilidad de distintas políticas de validez. (a) Tiempo de vida promedio de los grupos empleando distintas políticas de validez. (b) Razón de desintegración debida a invalidaciones. . . . .	85
4.5.	Costo del mantenimiento de redes jerárquicas construidas por diferentes políticas de validez. (a) Tasa de reafiliaciones promedio debida a la movilidad de los miembros. (b) Tasa de reafiliaciones promedio por invalidaciones de grupos por política estricta. (c) Función de autocorrelación (FAC) del número de reafiliaciones. (d) Traza del número de reafiliaciones producidas en una red de 300 nodos bajo la configuración antes mencionada. . . . .	88

# Capítulo 1

## Introducción

Actualmente, los usuarios de dispositivos móviles necesitan de la infraestructura de red convencional para explotar la gran versatilidad de opciones de comunicación que tienen, p. ej. telefonía celular, mensajería instantánea, correo electrónico y *microblogging*, por citar algunos. Generalmente, estos servicios pueden emplearse sin ningún percance, no obstante, existen casos en donde los dispositivos móviles pierden su capacidad de comunicación debido a que la infraestructura de red falla, no está disponible o su acceso es costoso. El primero corresponde a zonas donde la infraestructura ha sido dañada por la acción de alguna catástrofe. El segundo es característico de las zonas rurales, montañosas, o de países en desarrollo, donde las redes de comunicación no ofrecen una cobertura amplia. El tercero se presenta cuando los usuarios no desean conectarse a la infraestructura de red debido a que el precio por el servicio les resulta elevado.

En los casos antes descritos, las comunicaciones pueden habilitarse mediante el establecimiento de *redes ad hoc móviles* (*mobile ad hoc network*, MANET). Técnicamente, estos sistemas son una infraestructura de comunicación descentralizada y formada bajo demanda que se compone únicamente de dispositivos móviles que se interconectan inalámbricamente sin la

intervención de agentes externos. Estos dispositivos, denotados como *nodos*, tienen dos funciones: la de terminal de usuario y la de encaminador. La última es esencial ya que los nodos con tal función establecen rutas multisalto que permiten la comunicación entre los que no son directamente enlazables. Con base en esta organización, las redes ad hoc móviles proveen teóricamente los servicios de red que las aplicaciones distribuidas necesitan para poder ser ejecutadas [1, 2].

Las características de descentralización y autoorganización propias de las redes ad hoc móviles han motivado la utilización el modelo de red *par a par* [3–5] (*peer-to-peer*, P2P) como base para la ejecución de aplicaciones distribuidas en las que los nodos participan entre sí, de manera descentralizada y autoorganizada, en la gestión de los servicios que ofrecería un servidor de aplicaciones. De esta manera, son los participantes de la red P2P quienes prestan los servicios que emplean. Siguiendo el modelo P2P han surgido varias aplicaciones exitosas, p. ej. Spotify [7], Skype [8] y BitTorrent [9].

Debido a su naturaleza distribuida, en las redes P2P se requiere de un *servicio de búsqueda* que se encargue de descubrir la identidad de los nodos que ofrecen recursos. Esta función es muy relevante ya que de ella dependen otros servicios más complejos. Para llevarla a cabo pueden emplearse distintas técnicas de búsqueda que se clasifican en búsqueda no estructurada, estructurada y jerárquica [10]. Las redes P2P Gnutella v0.4 [11], Kademia [13] y Gnutella v0.6 [14] son ejemplos que corresponden respectivamente a cada una de las categorías anteriores.

Aunque las redes ad hoc móviles sirven de sustrato para la ejecución de aplicaciones distribuidas, no es posible establecer eficientemente sobre ellas una red P2P como las que se ejecutan sobre la Internet. La razón de esto es que dichas redes no incluyen estrategias que les permitan adaptarse a las características propias de las redes ad hoc móviles, tal como se describe a continuación.



---

El diseño original de las redes P2P no acota el caudal de datos (*throughput*), porque la infraestructura de comunicaciones no tiene limitantes en ese aspecto. Por esta razón, este tipo de red P2P no operaría correctamente en redes ad hoc móviles donde el caudal de datos es bajo porque las comunicaciones entre nodos móviles se efectúan generalmente sobre un mismo canal inalámbrico. Específicamente, el caudal de datos  $C$  por nodo está acotado por  $\Theta(C/\sqrt{N})$  [15], donde  $N$  es el *tamaño de la red*, es decir, el número de nodos que la integra. Esta característica hace que los protocolos ejecutados en redes ad hoc móviles deban ser eficientes, limitando los mensajes de control que requieren para funcionar. De lo contrario, obstaculizarían la operación de otros protocolos y de las aplicaciones de usuario.

Además de lo anterior, las redes P2P son redes lógicas (*overlays*), que no poseen mecanismos para tratar con la movilidad de los nodos que conforman la ruta donde se establece un enlace lógico. Únicamente, están diseñadas para tratar con los cambios topológicos generados por el fenómeno de la rotación de los participantes de la red P2P (*churn*), el cual es provocado por los inicios y cierres de sesión de miles, inclusive millones de usuarios [16].

Con el fin de atender las cuestiones anteriores, se han presentado varias propuestas que a continuación se enlistan de acuerdo con el tipo de técnica de búsqueda que emplean.

**Búsqueda no estructurada** Basada en el protocolo de inundación, esta técnica ha sido adaptada a las redes ad hoc móviles y ha demostrado ser eficaz en escenarios donde el grado de movilidad de los nodos es alto [17–19]. Los servicios basados en esta técnica tienen la característica de ser económicos de mantener ya que se ejecutan hasta ser requeridos, por lo que sólo emplean mensajes de mantenimiento de vecindarios locales. La búsqueda no estructurada puede realizarse sobrecargando el funcionamiento de algunos protocolos de encaminamiento para redes ad hoc móviles, tal como se hace en [18]. La desventaja principal de estas propuestas es que su costo en comunicaciones es de  $\mathcal{O}(N^2)$ , donde  $N$  es el tamaño

de la red.

**Búsqueda estructurada** Esta estrategia está basada en tablas *hash* distribuidas y tiene la ventaja de usar pocos nodos para resolver la petición por un recurso, como se muestra en [20–26]. Bajo esta estrategia, los nodos organizan una red lógica que se establece en la capa de aplicación. Su topología está diseñada para descubrir la identidad de los prestadores de recursos de manera determinista. Al establecerse en la capa de aplicación, la topología lógica de estas redes generalmente no empata con la física, lo que ocasiona que la resolución de consultas emplee muchos más mensajes que los que meramente necesita. Para resolver este problema, las tablas *hash* distribuidas se modificaron para ser ejecutadas en la capa de red [20, 22–25, 27] o para comunicarse con ésta mediante una capa vertical de variables compartidas [26]. No obstante, el costo de ofrecer este servicio puede ser elevado si los enlaces lógicos cambian abruptamente porque se requerirían muchos mensajes de control para mantener la conectividad lógica de la estructura distribuida. Con base en esta observación, en [28] se menciona que las redes lógicas sólo pueden prestarse en escenarios donde los nodos exhiben baja velocidad.

**Búsqueda jerárquica** Se ejecuta sobre una red lógica integrada por grupos de nodos, cada uno de ellos organizado por un líder que gestiona el índice de los recursos que comparten sus nodos afiliados. Así, el servicio de búsqueda es provisto por el conjunto de líderes, los cuales se encargan de resolver, en primera instancia, las solicitudes que provienen de su grupo y, en segunda instancia, las que no pudieron ser resueltas localmente en otros grupos. La búsqueda jerárquica resulta más eficiente que la búsqueda por inundación ya que una consulta se resuelve contactando a todos líderes en el peor caso. De hecho, esta técnica ha sido empleada por protocolos de encaminamiento y ha mostrado un buen desempeño con respecto a otras estrategias [29, 30]. No obstante, es susceptible a la movilidad ya que la

---

composición de los grupos se modifica conforme los nodos se mueven. Esto hace que la red lógica tenga enlaces incorrectos y, en consecuencia, que el servicio de búsqueda presente problemas de desempeño. Para mantener la funcionalidad de la red, los nodos intercambian mensajes de control de manera proactiva, incrementándose así el costo de la búsqueda [31].

Los servicios ejecutados en redes ad hoc móviles deben considerar el caudal de datos limitado y la topología dinámica de la infraestructura de comunicación para operar correctamente. Consecuentemente, el servicio de búsqueda, el cual es la función nuclear de toda aplicación P2P, debería ofrecerse por medio redes estructuradas o jerárquicas que son eficientes porque su servicio de búsqueda resuelve consultas con pocos mensajes. Además, su protocolo de autoorganización debe diseñarse para adaptar la topología lógica de la red P2P a las características topológicas de las redes ad hoc móviles, las cuales dependen de los patrones de movilidad de las entidades que las integrarían potencialmente: humanos. De lo contrario, la eficiencia obtenida por ofrecer un servicio de búsqueda estructurado o jerárquico se perdería porque el protocolo de autoorganización sobrecargaría la red con mensajes de control.

En la literatura, se han presentado distintas propuestas de servicios de búsqueda que aparentemente hacen frente a los retos que las redes ad hoc móviles imponen. No obstante, ninguna de ellas se basa en las características que exhibiría una red formada por dispositivos móviles portados por humanos. De hecho, casi todas ellas se basan en un conjunto de restricciones que no corresponden a las propiedades de la movilidad humana reportadas en [32–34] y [35]. Esto hace que no sea posible asegurar que las soluciones actuales funcionen eficientemente en redes ad hoc móviles. Además, ninguna de ellas se beneficia del conocimiento generado del análisis de redes P2P diseñadas para la Internet, específicamente de aquel que hace que estas redes operen correctamente. Con base en estas observaciones, se plantea el siguiente problema de investigación.

## 1.1. Problema de investigación

Los servicios ejecutados en redes ad hoc móviles deben diseñarse a la medida de la infraestructura de comunicaciones, es decir, deben operar en una red con topología dinámica y caudal de datos limitado. Aunque existen varias redes P2P que prestan el servicio de búsqueda, ninguna se ajusta a las características estadísticas que las redes ad hoc móviles exhibirían potencialmente al considerar que se conforman por los dispositivos móviles que portan los humanos, tal como se asume generalmente en la literatura. Además, las lecciones del paradigma P2P sobre la Internet no se toman en cuenta en el diseño de las propuestas existente. En consecuencia, no es posible asegurar que las soluciones provistas hasta ahora operen eficientemente en el ambiente en cuestión. Por ello, en esta tesis doctoral se plantea la siguiente pregunta de investigación: ¿Qué estrategias permiten establecer redes estructuradas y jerárquicas de manera eficiente sobre redes ad hoc móviles?

## 1.2. Objetivo general

*Determinar estrategias que permitan la ejecución eficiente de redes jerárquicas o estructuradas sobre redes ad hoc móviles.*

## 1.3. Objetivos particulares

I *Determinar estrategias que hacen que las tablas hash distribuidas operen exitosamente sobre topologías de red dinámicas con infraestructura fija.* La finalidad de este objetivo es identificar las estrategias que permiten que el servicio de búsqueda prestado por las tablas *hash* distribuidas sea confiable y eficiente en ambientes dinámicos.

II *Determinar características estadísticas de la topología de red inducida por un modelo de movilidad humana.* En la literatura [36–38], se ha demostrado que la eficiencia de los protocolos de redes ad hoc móviles depende en buena medida de la manera en que el movimiento de los nodos se representa. Además, la operación correcta de redes P2P estructuradas depende de que se consideren las características que vuelven a la red dinámica [40]. Dado que los dispositivos móviles son portados por humanos, conviene analizar las características topológicas de las MANET bajo un modelo que represente con mayor detalle el movimiento humano. Esto con la finalidad de definir las estrategias que soportarían el mantenimiento de una red estructurada o jerárquica.

III *Determinar estrategias que mantengan la organización de las redes lógicas de tipo jerárquico.* Alcanzar este objetivo permite identificar qué reglas de organización hacen que las estructuras de grupos sean *estables*, es decir, que mantengan su formación a pesar de los cambios de conectividad de las redes ad hoc móviles.

## 1.4. Metodología general

Para alcanzar los objetivos se realizan los siguientes procedimientos generales:

1. Identificación y comprensión de la literatura científica relacionada con las redes ad hoc móviles, redes P2P y servicios de búsqueda.
2. Desarrollo de herramientas de simulación que permitan la experimentación con redes ad hoc móviles.
3. Desarrollo de marcos de evaluación que permitan la comparación justa entre los algoritmos de interés para esta investigación.
4. Análisis experimental de protocolos ejecutados en redes P2P y redes ad hoc móviles.

## 1.5. Lista de contribuciones

Del desarrollo de esta tesis doctoral se produjeron los siguientes artículos de investigación:

1. Artículo titulado «*Studying the Effect of Human Mobility on MANET Topology and Routing: Friend or Foe?*» [39] presentado en la conferencia internacional MobiWac'15 y publicado en las memorias de dicho foro. En este trabajo se presentan los resultados y el análisis de haber observado las características de la topología física de las redes ad hoc móviles bajo un modelo que representa varias propiedades de la movilidad humana.
2. Artículo titulado «*A performance comparison of Chord and Kademia DHTs in high churn scenarios*» [40] publicado en la revista internacional indexada *Peer-to-peer Networking and Applications*. En éste se presentan las lecciones que deben de ser tomadas en cuenta para que las tablas *hash* distribuidas Chord y Kademia operen en redes lógicas dinámicas de manera *confiable*.
3. Artículo titulado «*On the effect of peer online times on the lookup service of Chord and Kademia P2P systems*» [41] presentado en la conferencia internacional IEEE LATIN-COM 2013 y publicado en las memorias de dicho foro. En el artículo se presenta un análisis sobre la cantidad de usuarios fijos que se necesitan para mejorar el desempeño de las tablas *hash* distribuidas Chord y Kademia.

Además de lo anterior, se realiza una evaluación de estrategias estabilizantes de protocolos de agrupamiento. Del análisis de los resultados de esta evaluación se identifican las estrategias que aumentan la *estabilidad* de protocolos de agrupamiento para redes ad hoc móviles.

Finalmente se presenta una implementación sintética del modelo de caminata autosimilar de menor acción (*self-similar least-action walk model*, SLAW [32]) en el simulador INET [42], el cual se basa en OMNeT++ [43].

En resumen, a través de esta tesis doctoral se presentan: (1) estrategias identificadas de la evaluación de tablas *hash* distribuidas en redes lógicas con topología dinámica, (2) características estadísticas que las redes ad hoc móviles exhiben cuando el movimiento de los nodos corresponde a las propiedades de la movilidad humana, y (3) estrategias estabilizantes que hacen que las redes lógicas de tipo jerárquico mantengan su formación tanto como sea posible.

## 1.6. Estructura de la tesis

Esta tesis doctoral se desarrolla siguiendo esta estructura. En el capítulo 2, se determinan las estrategias que hacen que las tablas *hash* distribuidas operen exitosamente en redes lógicas dinámicas con infraestructura fija. Enseguida, en el capítulo 3, se presentan y analizan las características estadísticas de las redes ad hoc móviles bajo el modelo de movilidad SLAW. Después, en el capítulo 4, se determinan las estrategias que vuelven a las estructuras de agrupamiento estables ante la movilidad. Finalmente, en el capítulo 5, se enuncian las conclusiones y perspectivas de este trabajo de investigación.





## Capítulo 2

# Lecciones aprendidas de redes P2P estructuradas con infraestructura

Las redes ad hoc móviles y las P2P diseñadas para la Internet presentan características similares y retos comunes. Con base en sus definiciones, los servicios prestados por las primeras son diseñados de manera descentralizada, al igual que los provistos por las redes P2P. Además, los protocolos ejecutados en ambos tipos de redes se diseñan para ser *confiables*, es decir, para operar correctamente, dentro de sus parámetros de diseño, en una red cuya conectividad cambia continuamente. Es por estas similitudes que los mecanismos sobre los que reside la confiabilidad de las redes P2P convencionales pueden tomarse como base para el diseño de un protocolo de búsqueda para redes ad hoc móviles.

Las *tablas hash distribuidas* son una clase de sistema distribuido descentralizado muy popular para establecer redes P2P debido a su eficiencia para resolver búsquedas. Específicamente, son estructuras de datos donde los usuarios almacenan duplas del tipo  $\langle key, value \rangle$ , las cuales representan recursos compartidos. En dichas duplas, *key* es la clave *hash* de un recurso compartido y *value* es la dirección IP y el puerto UDP del nodo que comparte dicho recurso,

p. ej. si  $\text{hash}(\text{doc.pdf}) = 12345$ , entonces una posible dupla sería  $\langle 12345, 192.168.0.1:4567 \rangle$ . Estas estructuras son creadas mediante la distribución de los fragmentos de una tabla *hash* entre todos los nodos que pertenecen a la red P2P. Para esto, los nodos establecen enlaces lógicos entre sí que conectan los fragmentos de la tabla *hash* siguiendo reglas de proximidad que conllevan a la formación de topologías de red como anillos, árboles o hipercubos, todas ellas superpuestas a la Internet. Esta organización topológica permite que la búsqueda por un recurso se resuelva de manera determinista, en el peor de los casos con  $\mathcal{O} \log(N)$  mensajes, donde  $N$  es el tamaño de la red. Esta característica hace que teóricamente las tablas *hash* distribuidas puedan dar servicio a un gran número de usuarios porque requieren de una cantidad sublineal de mensajes para operar. En el caso de las redes ad hoc móviles, esto significaría que las solicitudes por recursos podrían encaminarse directamente al nodo que almacena la dupla que permite localizar al destino en la topología lógica, tal como se hace en [22–27].

En la literatura, se han propuesto diversas maneras de establecer redes P2P [6], no obstante este estudio se centra en *tablas hash distribuidas* porque éstas pueden desempeñarse bien en redes donde las conexiones lógicas cambian abruptamente debido a la *rotación de los participantes* (*churn* [16]). En el contexto de esta tesis se evalúan las tablas *hash* distribuidas Chord [12] y Kademlia [13] porque han sido un objeto popular de investigación y desarrollo, tanto por parte de la academia como de la industria: Chord forma parte de la primera generación de tablas *hash* distribuidas y ha sido evaluado en varias investigaciones debido a su disponibilidad y simplicidad mientras que Kademlia es el sustrato de búsqueda descentralizada empleado por el protocolo BitTorrent, el cual tiene una gran cantidad de usuarios.

Para alcanzar el objetivo particular de determinar las estrategias que hacen que Chord y Kademlia operen exitosamente sobre topologías de red dinámicas, se estudia el funcionamiento

de las tablas *hash* distribuidas en cuestión (sección 2.1). Enseguida, se define un marco de evaluación de tablas *hash* distribuidas (sección 2.2) con el que se obtienen los resultados explicados en la sección 2.3. Después, se presenta una discusión sobre los mecanismos que pueden ser empleados como base para prestar servicios de búsqueda P2P basados en tablas *hash* distribuidas para redes ad hoc móviles (sección 2.4). El contenido presentado en esta sección es preliminarmente descrito en [44] y posteriormente refinado en los artículos publicados en [40, 41].

## 2.1. Tablas hash distribuidas

Las tablas *hash* distribuidas pueden ser definidas en términos de su *espacio de claves*, del *estado de los nodos*, su *protocolo de búsqueda* y su *protocolo de autoorganización*. El espacio de claves es simplemente el conjunto de identificadores empleados para diferenciar tanto a los nodos que conforman la red P2P como a los recursos compartidos. Generalmente, se compone de cadenas de bits de longitud fija  $m$ , por lo tanto el número cardinal de este conjunto es  $2^m$ . El estado de los nodos se compone de un conjunto de referencias que se almacenan para resolver las solicitudes por recursos. Usualmente, se requiere de  $\mathcal{O} \log(N)$  referencias para soportar el servicio de búsqueda, donde  $N$  es el tamaño de la red. Además, los nodos almacenan las referencias de recursos con clave próxima a su identificador. El protocolo de búsqueda es el conjunto de reglas que los nodos siguen para explorar la topología lógica de la red con el objetivo de descubrir un recurso compartido. A su vez, el protocolo de autoorganización es el conjunto de reglas que los nodos obedecen para mantener la topología de la red sin enlaces inválidos.

### 2.1.1. Chord

El espacio de claves de Chord es un conjunto de cadenas de bits que se organiza de manera ascendente para formar un anillo. Así, la clave más grande tiene por sucesor a la clave más pequeña. En la figura 2.1 se ilustra un espacio con claves de tamaño  $m = 8$ .

El estado de nodos se compone de varias estructuras de datos y una referencia hacia el predecesor inmediato. La primera estructura es un repositorio donde se mantienen las duplas de los recursos compartidos. Los nodos son responsables de almacenar las claves de los recursos que se encuentran entre su propia clave y la clave del nodo que lo precede, p. ej., el nodo 146 de la figura 2.1 tiene que almacenar todas las duplas que pertenezcan al intervalo  $(128, 146]$ . La segunda estructura es una lista de claves llamada *lista de sucesores* que almacena en el peor de los casos  $\mathcal{O} \log(N)$  duplas de los nodos con clave inmediatamente superior. En el caso del nodo 146, la lista contendría las duplas de los nodos cuya clave está entre 160 y 18. La última es una tabla de atajos (*finger table*) que contiene referencias que conducen hacia los sucesores de las claves que se encuentran a una distancia de  $2^i$ , donde  $i \in [0, m)$ . La tabla de atajos del nodo 146 se ilustra en la figura 2.1. En el ejemplo, y siendo  $\text{mod}(x, y)$  la función que regresa el módulo de  $x$  con respecto a  $y$ , puede notarse que cada entrada de la tabla de atajos almacena la clave del sucesor que corresponde a  $\text{mod}(146 + 2^i, 2^8)$ .

El protocolo de búsqueda de Chord tiene por objetivo encontrar al sucesor de la clave que le

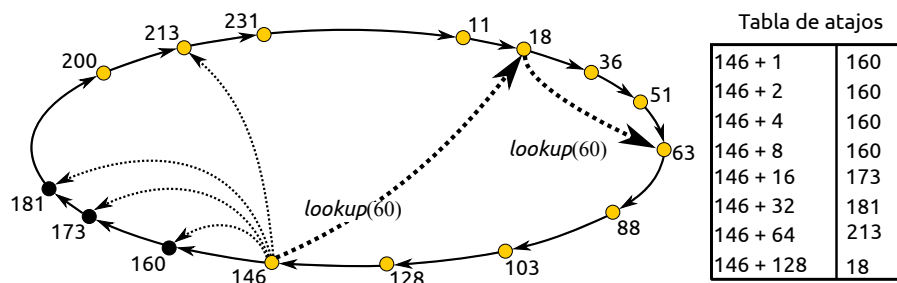


Figura 2.1: Espacio de claves y tabla de atajos del nodo 146.

es dada como argumento, para ello se siguen dos estrategias. La primera consiste en emplear la lista de sucesores para transmitir las solicitudes de manera secuencial y dextrógira hasta alcanzar al sucesor de la clave buscada. Este esquema de búsqueda tiene una complejidad de mensajes  $\mathcal{O}(N)$ , lo cual no es escalable para una red con  $N$  muy grande. Para acelerar las búsquedas, los nodos emplean las referencias contenidas en la tabla de atajos. Así, las consultas se reenvían al nodo más próximo al sucesor de la clave solicitada. Este esquema de búsqueda tiene una complejidad de  $\mathcal{O} \log(N)$  ya que la distancia entre el solicitante y el destino se reduce al menos a la mitad en cada reenvío. En el ejemplo ilustrado en la figura 2.1, se muestra que el nodo 146 realiza una búsqueda por la dupla con clave 60 que es administrada por el nodo 63. Usando la tabla de atajos, el nodo 146 determina que el nodo 18 es el más cercano al sucesor de la clave 60. Siendo así, el nodo 146 solicita al 18 la clave 60. Después, el nodo 18 emplea su lista de sucesores para notar que el nodo 63 es quien tiene la dupla con clave 60. Así, el nodo 18 reenvía la consulta al nodo 63, quien dará respuesta a la consulta original.

Los nodos preservan el anillo lógico ejecutando el siguiente protocolo de autoorganización. Este establece las acciones a seguir para reparar los enlaces lógicos inválidos producidos por los inicios y cierres de sesión de los participantes.

El mantenimiento de la red se hace verificando que las entradas en la lista de sucesores sean correctas. Para ello, se lleva a cabo una rutina llamada *estabilización* que consiste en solicitar a cada uno de los nodos que integran la lista de sucesores la identidad de su predecesor. La ejecución de esta rutina es periódica y se realiza en segundo plano. No obstante, la rutina también puede ser invocada explícitamente cuando se encuentran errores en la lista al momento de servir búsquedas. La tabla de atajos se actualiza de forma reactiva ya que resultaría muy costoso darle mantenimiento con la misma frecuencia que la lista de sucesores debido a la manera en la que se construye.

La unión de nodos nuevos se efectúa como sigue. Como primer paso, un nodo nuevo calcula el identificador que le corresponde del espacio claves de Chord. Esto lo hacen usando una función *hash* consistente, como la SHA-1 [45]. Enseguida, el nodo nuevo solicita el valor de su propia clave a un nodo que ya forma parte del anillo. Esta búsqueda tendrá como resultado la dupla del sucesor del nodo nuevo. Con esta información, el recién llegado contacta a su sucesor y le solicita su lista de sucesores y el rango de duplas que debe gestionar. Al recibir esta solicitud, el sucesor del nodo nuevo actualiza la referencia de su predecesor. Después, el nodo nuevo llena su tabla de atajos solicitando la clave del sucesor que corresponde a la entrada de dicho contenedor. Una vez que el nodo nuevo completó su estado sólo espera a que su predecesor ejecute la rutina de estabilización para quedar completamente unido al anillo.

Finalmente, los nodos cierran su sesión transfiriendo sus duplas a su nodo sucesor e indicándole la clave del predecesor que le corresponderá. Después de eso, se le pasa al predecesor la clave de su nuevo sucesor y así el anillo se cierra excluyendo al nodo que se retira.

### 2.1.2. Kademlia

Como se observa en la figura 2.2, el espacio de claves de Kademlia se organiza como un árbol binario completo cuyas hojas son cadenas binarias de  $m$  bits, por omisión  $m = 160$  bits, y cuyos nodos intermedios corresponden al prefijo común que poseen dos nodos del mismo padre. En esta figura, los vértices sin color representan claves sin ser asignadas. La proximidad entre dos claves se determina por el resultado numérico que se obtiene de aplicarles la función lógica XOR. Así, dos claves son próximas si su diferencia numérica es pequeña. De hecho, mientras mayor sea la longitud del prefijo común que compartan dos claves, menor será su diferencia. Por lo tanto, las claves más próximas son las que sólo difieren en su bit menos significativo. En la figura 2.2 también es posible notar que todas las claves que poseen  $i$  bits

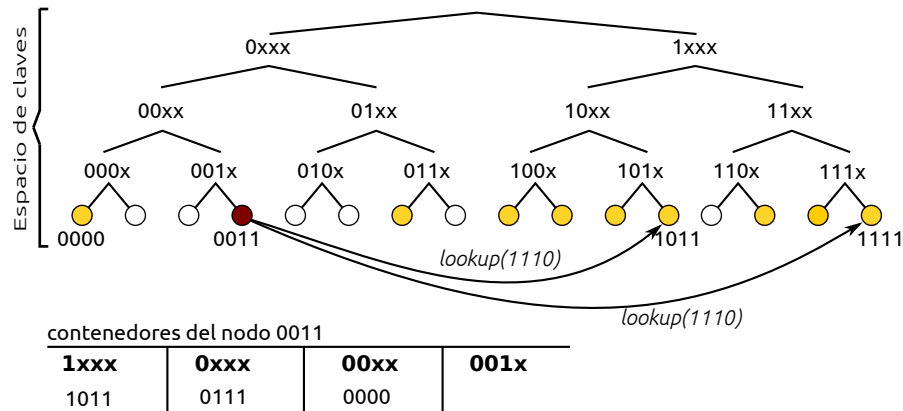


Figura 2.2: Espacio de claves de Kademlia con longitud  $m = 4$  bits y contenedores de longitud  $k = 1$  del nodo 0011.

de prefijo en común pertenecen al mismo subárbol de nivel  $i$ , donde  $i \in [1, m)$  es el nivel del árbol binario.

En Kademlia, los nodos guardan duplas en *contenedores* (*buckets*) de longitud  $k$ . Los nodos mantienen en total  $m$  contenedores, uno por cada subárbol de nivel  $i$ . Específicamente, los nodos almacenan en el primer contenedor claves de nodos con los que no comparten ningún bit en el prefijo y en el  $m$ -ésimo contenedor almacenan, de existir, la clave del nodo con la máxima similitud de prefijo, es decir  $m - 1$  bits, de acuerdo con el criterio de proximidad de la operación XOR. Esto se ilustra en la figura 2.2, donde el nodo 0011 tiene almacenado en su primer contenedor al nodo con clave 1011, con el cual no tiene similitud en prefijo. Este mismo nodo no tiene almacenada ninguna entrada en el contenedor número cuatro porque ningún nodo ha tomado la clave 0010. Otra característica de los contenedores es que sus entradas se ordenan de acuerdo al tiempo en que fueron recibidas. Esto para realizar las búsquedas con base en los nodos que han sido recientemente vistos ya que es muy probable que ellos permanezcan en el sistema por más tiempo [13, 16]. De acuerdo con sus autores, Kademlia está diseñado para asegurar que los nodos tengan al menos una entrada en cada uno de sus contenedores. Además de la información para resolver búsquedas, los nodos guardan las duplas de los recursos compartidos con clave próxima a la suya. En adición, los nodos

mantienen en *caché* las duplas que han reenviado como respuesta a una petición.

Los nodos resuelven las consultas por recursos ejecutando el siguiente protocolo de búsqueda. Como primer paso, un solicitante busca en sus contenedores  $\alpha$  duplas con clave próxima a la del recurso solicitado, donde  $\alpha$  es un parámetro configurable que determina el número de consultas a lanzar. En el caso ilustrado en la figura 2.2, el nodo 0011 está buscando al nodo con clave 1110, entonces, si suponemos  $\alpha = 1$ , el solicitante envía al nodo 1011 la solicitud por la dupla de 1110. Después, el solicitante envía de manera asíncrona una petición por el recurso a cada uno de los nodos que corresponden a la dupla. Los receptores pueden responder de dos maneras. La primera es reenviando la dupla solicitada si es que la conocen. La segunda es enviando al solicitante  $k$  duplas con claves próximas al objetivo. Si el solicitante recibe la dupla que buscaba, entonces la búsqueda finaliza. De lo contrario, el solicitante vuelve a ejecutar el proceso de búsqueda tomando de las respuestas que recibe  $\alpha$  duplas con claves de nodos no consultados anteriormente. Esto se hace tan pronto como recibe una respuesta y hasta que el proceso da con el objetivo o falla. Debido a la organización lógica de Kademlia, las respuestas contendrán duplas con claves más próximas al objetivo en comparación con las que el solicitante tiene originalmente. De hecho, la distancia lógica entre las claves recibidas y la clave objetivo se reduce a la mitad en cada respuesta. En el caso ilustrado en la figura 2.2, el nodo 0011 recibe del nodo 1011 la dupla del nodo con clave 1111, la cual es la más próxima al objetivo que se busca. Entonces, la búsqueda ilustrada en la figura 2.2 terminará una vez que el nodo 0011 consulte al nodo 1111 ya que éste tiene en sus contenedores la dupla del nodo 1110.

El protocolo de autoorganización de Kademlia establece las reglas para mantener actualizado el estado de los nodos y también determina el procedimiento mediante el cual los nodos nuevos se unen a la red. No obstante, no tiene reglas directas para atender las salidas de los nodos. A continuación se presenta su funcionamiento.



Para hacer frente a los cambios de conectividad, el estado de los nodos se corrige mediante la ejecución de una *rutina de actualización (refresh)* que comprueba si un nodo elegido aleatoriamente sigue en línea. Además, se aprovecha el tráfico de red para actualizar los contenedores ya que la recepción de una respuesta indica que un nodo consultado sigue en línea. En adición, a las respuestas se les adjunta un mensaje PING con el que los nodos que atendieron una consulta obtienen la dupla del nodo que hizo la consulta; esto se conoce como *acarreo a cuestas (piggybacking)*. Otra regla establecida por el protocolo indica que cada entrada de los contenedores se mantenga hasta que el nodo al cual hace referencia deje de estar en línea.

El protocolo de autoorganización establece las siguientes reglas para unir nodos nuevos a la red lógica. Para empezar, un nodo nuevo debe calcular su clave, para esto usa alguna función *hash* conocida por todos los nodos de la red. Después, el nodo nuevo busca la dupla que corresponde a la clave que calculó a través de otro ya conectado a la red. Durante el proceso, el nodo nuevo recibirá información para llenar sus contenedores debido al mecanismo de acarreo a cuestas. Además, el nodo nuevo es insertado únicamente en aquellos contenedores con entradas libres ya que el estado de los nodos no se modifica con la llegada de participantes nuevos. El proceso finaliza cuando la dupla del recién llegado queda publicada en los  $k$  nodos con clave más próxima.

## 2.2. Marco de evaluación

En esta sección se detallan las características del marco de evaluación empleado para medir el nivel de confiabilidad de las tablas *hash* distribuidas y la cantidad de mensajes de control que requieren para operar en dos escenarios: uno donde existe un nivel alto de rotación de los participantes y otro donde existen participantes que no cierran su sesión. Además, se

presentan las medidas de desempeño y el conjunto de procedimientos llevados a cabo para hacer la evaluación.

### 2.2.1. Modelado de la rotación de los participantes

La topología de las redes P2P cambia con respecto al tiempo debido al fenómeno de la rotación de los participantes: inicios y cierres de sesión de miles, inclusive millones, de usuarios de una red P2P. Modelar este fenómeno teniendo en cuenta la evidencia tomada de sistemas reales [16] ha hecho posible que modelos teóricos basados en procesos de Poisson (emplados en [46, 47]) o procesos de fallas aleatorias (usados en [48–50]) sean sustituidos por modelos on/off (utilizados en [51, 52]) que representan mejor este fenómeno. La precisión de las características del fenómeno de la rotación conlleva a obtener resultados de desempeño más apegados a la realidad.

Los modelos on/off generan inicios y cierres de sesión considerando el comportamiento individual de los nodos. Para este fin, la participación de los nodos se modela mediante dos variables aleatorias  $T_{\text{on}}$  y  $T_{\text{off}}$  que son usadas para representar el tiempo en línea y el tiempo fuera de línea de los nodos, respectivamente. Así, un nodo deja la red cuando el tiempo muestreado de la variable aleatoria  $T_{\text{on}}$  expira. De igual forma, cada nodo inicia sesión nuevamente después de que un período de tiempo muestreado de la variable aleatoria  $T_{\text{off}}$  expira. Por motivos de simplicidad, las variables  $T_{\text{on}}$  y  $T_{\text{off}}$  se toman de la misma función de distribución, usualmente una de cola pesada [16, 53].

Generalmente, en los modelos on/off se emplea el tiempo de sesión medio  $\overline{T_{\text{on}}}$  para establecer el nivel de variabilidad en la conectividad lógica de la red. Así, mientras menor sea el tiempo de vida medio de las sesiones, mayor es la frecuencia de los cambios de la topología de la red. No obstante, esta medida no cuantifica directamente el nivel de la variabilidad de la

conectividad porque no está relacionada directamente con la red. Por ejemplo, un tiempo de sesión medio de 600 s no indica directamente el número de enlaces modificados en una ventana de tiempo dada.

Para atender esta cuestión, el nivel de variabilidad de la conectividad se mide por la *tasa de rotación normalizada* [40]. Esta medida se define como el porcentaje de cambios que experimenta el conjunto de participantes que integra una red P2P por unidad de tiempo. La medida se calcula de acuerdo con la siguiente fórmula:

$$R_c = \frac{100}{I\tau} \sum_{i=1}^I \frac{A_i + D_i}{S_i} \quad (2.1)$$

donde  $R_c$  es la razón de rotación normalizada (*normalized churn rate*),  $\tau$  es la duración de una ranura de tiempo  $i$ ,  $A_i$  y  $D_i$  son respectivamente el número de inicios y cierres de sesión ocurridos durante la ranura  $i$ ,  $S_i$  es el tamaño de la red al inicio de una ranura de tiempo e  $I$  es el número total de ranuras que componen el periodo de observación. La unidad de esta medida es %churn/s.

En este marco de evaluación se emplea un modelo on/off para provocar el fenómeno de la rotación de los participantes. El nivel de rotación se calibra mediante la razón de rotación normalizada.

### 2.2.2. Medidas de desempeño

El nivel de confiabilidad de las tablas *hash* distribuidas se cuantifica con la medida *razón de búsquedas exitosas*, denotada por  $L_r$ , la cual es el resultado de la división del número de consultas resueltas con éxito entre el número total de consultas realizadas.

También se emplea la medida *punto de ruptura* [48] para comparar las tablas *hash* distribuidas. Esta medida es igual al nivel de rotación de los participantes  $r_0$  que hace que el nivel de confiabilidad, medido por la razón de búsquedas exitosas  $L_r$ , cruce el umbral de 0.5, es decir,  $r_0 \mid L_r(r_0) = 0.5$ . La explicación de dicho valor es la siguiente.

Suponga que todas las comunicaciones realizadas en una red de tamaño  $N$  no presentan ningún inconveniente. Después, suponga que la red se divide en dos subredes: una de tamaño  $\lfloor \beta N \rfloor$  y otra de  $\lceil (1 - \beta)N \rceil$ , donde  $\beta \in [0, 1]$  y  $N$  es el tamaño de la red. Dentro de cada subred las comunicaciones no sufren fallas, pero la comunicación entre las subredes no es posible. Entonces, la razón de búsquedas exitosas será igual a

$$L_r = 2\beta^2 - 2\beta + 1 \quad (2.2)$$

si suponemos que cada nodo realiza una búsqueda por cada uno de los demás y que el tamaño de la red  $N$  es grande. Por ejemplo, cuando  $\beta = 0.5$  se obtiene la mínima razón de búsquedas exitosas que es igual a 0.5. Bajo el escenario descrito, el punto de ruptura mide el nivel de rotación de los participantes que hace que cada nodo ya no pueda alcanzar  $N/2$  nodos en la red. Su unidad de medición es la misma que la usada para medir el nivel de rotación.

El costo de las comunicaciones se mide por la siguiente fórmula:

$$(messages/time)/peer \quad (2.3)$$

donde *messages/time* denota la cantidad de mensajes de control por unidad de tiempo que un participante *peer* transmite durante un experimento. Su unidad de medición es denotada como mps/peer. Con esta medida sólo se cuentan los mensajes de control cuya función es el mantenimiento de la tabla *hash* distribuida.

### 2.2.3. Metodología experimental

La evaluación de las tablas *hash* distribuidas se realiza considerando dos escenarios. En el primero, una red de 1000 nodos experimenta un alto nivel de rotación de participantes. En conjunto, los nodos establecen y mantienen una tabla *hash* distribuida que emplean para resolver búsquedas por recursos existentes en la red cada  $t_{\text{query}}$  segundos, donde  $t_{\text{query}}$  es una variable aleatoria distribuida normalmente con media  $\mu = 60$  s y desviación estándar  $\sigma^2 = 36$  s<sup>2</sup>. Los nodos consideran que su búsqueda falló si no encuentran la clave dentro de 10 s. El objetivo de este escenario es evaluar el desempeño de las tablas *hash* distribuidas ante el fenómeno de la rotación de los participantes para determinar los mecanismos que las vuelven exitosas en redes lógicas dinámicas.

Siguiendo el mismo esquema de generación de búsquedas, en el segundo escenario se modela una red de 1000 nodos compuesta por distintas clases de participantes. La finalidad de esto es determinar la fracción necesaria de nodos fijos para aumentar la confiabilidad de la red hasta cierto nivel ya que, hipotéticamente, esta medida de desempeño debería mejorar con la participación de nodos con tiempos de permanencia largos.

Los escenarios anteriormente descritos se implementan en el simulador de eventos discretos Oversim versión 20121206. Con esta herramienta, las simulaciones se realizan en tres fases. En la fase de inicio, el simulador agrega nodos a la red de manera secuencial cada  $t$  segundos, donde  $t$  es una variable aleatoria distribuida normalmente con parámetros  $\mu = 1/10$  s y  $\sigma^2 = 1/900$  s<sup>2</sup>. Una vez creados, los nodos establecen su tiempo de sesión  $T_{\text{on}}$ , medido en segundos, para después ejecutar el protocolo de autoorganización que corresponda a la tabla *hash* distribuida a evaluar. Cada vez que el tiempo de sesión de un nodo expira, el simulador encola un evento de creación de un nodo nuevo después de  $T_{\text{off}}$  segundos. Una vez que la red alcanza el tamaño configurado, se ejecuta una fase de transición que permite a los nodos actualizar sus conexiones lógicas. La duración de la fase de transición para este conjunto de

experimentos es de 10 minutos. Al finalizar la segunda fase, comienza la de medición a la que se le asigna un tiempo de dos horas. Nótese que el simulador está instrumentado para que el fenómeno de la rotación de los participantes comience desde la etapa de creación de la red; esto es un elemento clave de la evaluación de desempeño discutida en este capítulo.

Para simular a Chord y Kademlia se emplean las implementaciones provistas por el simulador, calibradas de acuerdo con las configuraciones mostradas en la tabla 2.1. Ahí, los tríos que corresponden a Chord son de la forma  $\langle s_d, ls, f \rangle$ , donde el parámetro  $s_d$  denota el tiempo entre estabilizaciones,  $ls$  es el tamaño de la lista de sucesores y  $f$  es el tiempo entre reparaciones de la tabla de atajos. Para el caso de Kademlia se emplean los tríos  $\langle \alpha, k, r \rangle$ , donde el parámetro  $\alpha$  es el número de búsquedas asíncronas,  $k$  es el tamaño de los contenedores y  $r$  el tiempo entre actualizaciones. Esta calibración se basa en los resultados previamente presentados en [41, 44], donde se realiza una evaluación paramétrica en la que se mide el desempeño de 16 configuraciones para Chord y 32 para Kademlia.

El modelo on/off de rotación de los participantes se calibra de la siguiente manera. La distribución de probabilidad que modela las variables  $T_{\text{on}}$  y  $T_{\text{off}}$  es Weibull con parámetro de forma 0.5. Los niveles de rotación de los participantes son  $\{0.125, 0.25, 0.5, 0.75, 1, 1.25, 1.5, 1.75, 2\}$  %churn/s. Estos provocan una tasa de rotación alta. De hecho, los valores extremos equivalen a calibrar el tiempo de sesión medio con valores aproximados de 2025 y 90 s.

Con el fin de ilustrar el nivel de rotación impuesto a la red, en la figura 2.3 (superior) se muestra el número de inicios y cierres de sesión acumulados en ventanas de tiempo de 50 s, obtenidos de calibrar el nivel de rotación de los participantes con una  $R_c$  de 0.125, uno y dos

Tabla 2.1: Configuración de las tablas *hash* distribuidas.

Estructura	Configuraciones
Chord	$\langle 5, 8, 30 \rangle, \langle 5, 16, 30 \rangle$
Kademlia	$\langle 1, 8, 600 \rangle, \langle 3, 8, 600 \rangle$

%churn/s. Ahí, se puede apreciar que una aparente razón de rotación normalizada pequeña produce un número considerable de cambios en la red. El límite más bajo que definimos para estos experimentos,  $R_c = 0.125$  %churn/s, produce cerca de 100 cambios por ventana de tiempo, la de  $R_c = 1$  %churn/s causa cerca de 550 cambios y la mayor  $R_c = 2$  %churn/s genera aproximadamente 1200 cambios. Estos números pueden hacer pensar que el tamaño de la red varía abruptamente bajo tales configuraciones, pero no es así. Para ilustrar este hecho, en la figura 2.3 (inferior) se exhibe una serie de tiempo del tamaño de la red que corresponde al período de observación del número de cambios en el conjunto de participantes. Ahí, se puede observar que, en todos los casos, el tamaño de la red no varía abruptamente. Esta estabilidad es debida a que las variables  $T_{on}$  y  $T_{off}$  del modelo de rotación on/off presentado en este marco de evaluación están configuradas con la misma distribución de probabilidad.

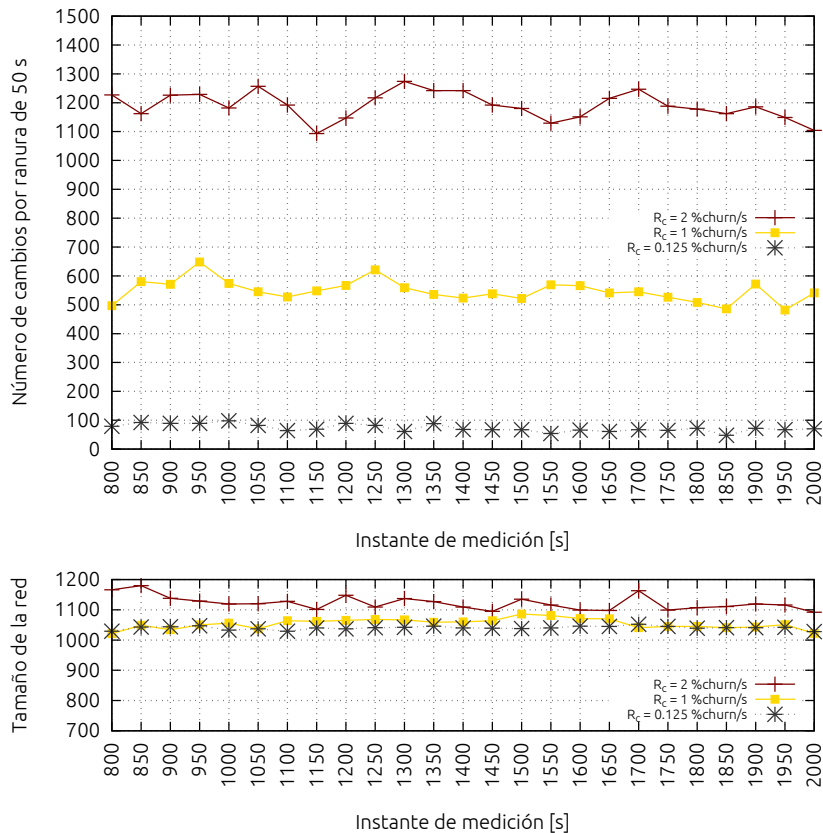


Figura 2.3: Representación gráfica de la rotación de los participantes.

También, la figura 2.3 permite observar que el tamaño de la red es mayor que 1000 nodos en todos los casos. Esto ocurre porque el simulador agrega nodos hasta que se alcanza un tamaño de red predeterminado. No obstante, el hecho de que se haya alcanzado dicho tamaño de red no implica que dejen de aparecer nodos nuevos debido a que el simulador encola la creación de los nodos que cierran sesión antes de que la fase de inicio termine.

La calibración de Chord y Kademlia para el segundo escenario se basa en las configuraciones del primer escenario que exhiben el peor desempeño en términos del nivel de confiabilidad. A su vez, el modelo de rotación de los participantes se calibra teniendo en cuenta que los nodos se pueden clasificar de acuerdo con el tiempo de sesión que exhiben [16, 54]. A los nodos que permanecen poco tiempo se les llama *mirones*, los que permanecen por lo menos el tiempo que se requiere para descargar completamente un archivo se les llama simplemente *participantes* y a los que están en línea durante tiempos extraordinariamente largos se les llama *benefactores*.

Con base en la clasificación de arriba se plantean las composiciones de red presentadas en la tabla 2.2. Específicamente, se analiza el caso en el que el tiempo de sesión de los participantes y mirones es de 1800 y 300 s, respectivamente. Este conjunto de configuraciones se etiqueta como *nivel medio*, ya que está diseñado para representar una red donde un recurso tarda aproximadamente 30 minutos en ser descargado. Además, se analiza un caso en el que se aumenta el nivel de rotación de los participantes y de los mirones a 934 y 92 s, respectivamente, lo que equivale a una tasa de rotación normalizada de uno  $\%churn/s$  para los primeros y dos  $\%churn/s$  para los segundos. Este último conjunto se etiqueta como *nivel alto*. En ninguno de los casos, los benefactores tienen un tiempo de sesión asignado porque ellos siempre están en línea, por lo que deberían contribuir en aumentar el nivel de confiabilidad de la red.



Tabla 2.2: Composición de red P2P heterogénea. Notación:  $\overline{T_{on}}$  es el tiempo en línea medio;  $C_n$  significa composición número  $n$ .

Tipo de nodo	Nivel medio (N1)			Nivel alto (N2)				
	$\overline{T_{on}}$ [s]	$C_1$	$C_2$	$C_3$	$\overline{T_{on}}$ [s]	$C_1$	$C_2$	$C_3$
<i>Benefactor</i> (Be)	–	0.3	0.2	0.1	–	0.3	0.2	0.1
<i>Participante</i> (Pe)	1800	0.6	0.6	0.6	934	0.6	0.6	0.6
<i>Mirón</i> (Pp)	300	0.1	0.2	0.3	92	0.1	0.2	0.3

## 2.3. Resultados

Chord y Kademia son estructuras que poseen mecanismos similares para dar soporte a la búsqueda de claves: en ambas es posible configurar el tamaño de la lista de sucesores y de los contenedores, al igual que la frecuencia con la que se corrigen sus entradas. No obstante, ambas exhiben desempeños diferentes como se muestra enseguida.

### 2.3.1. Evaluación en condiciones de cambio abruptas

En la figura 2.4(a), se muestra el nivel de confiabilidad exhibido por Chord y Kademia. Cada valor en la gráfica corresponde al promedio de 25 ejecuciones independientes del experimento. Las barras de error corresponden a intervalos de confianza del 95%. Ahí, puede notarse directamente que el desempeño de Kademia es superior al de Chord en cuestión de confiabilidad. En adición, en la figura se observa que la configuración de Chord  $\langle 5, 16, 30 \rangle$  presenta un punto de ruptura entre 1.2 %churn/s y la configuración  $\langle 5, 8, 30 \rangle$  de 1.4 %churn/s, lo cual se resalta por los cruces entre sus respectivas curvas de desempeño y la línea punteada. En contraste, las curvas de desempeño de Kademia no muestran un punto de ruptura. Por ello, puede enunciarse que Kademia ofrece un mayor nivel de confiabilidad que Chord en escenarios donde la tasa de rotación de los participantes es alta.

El nivel de confiabilidad de Chord se ve afectado severamente por dos razones. La primera es

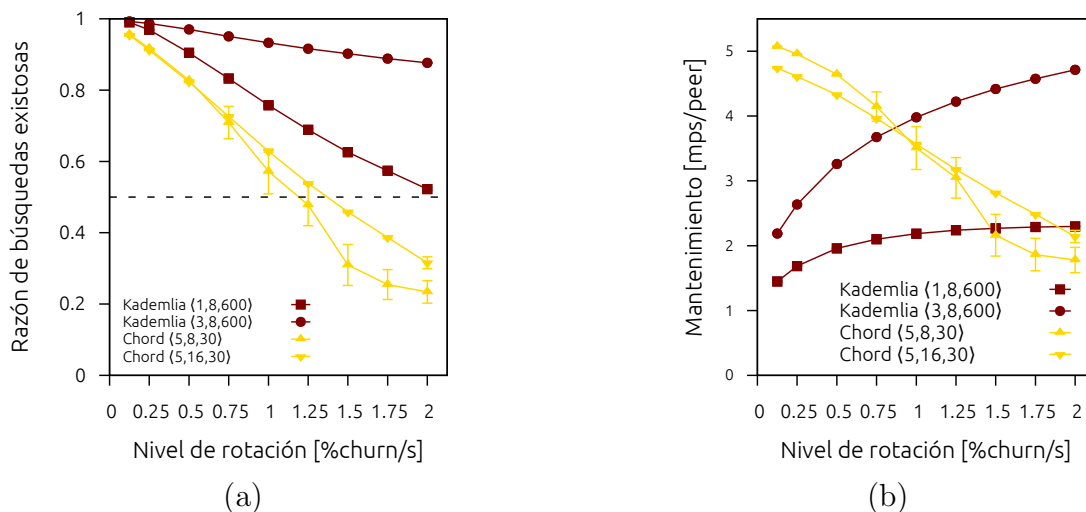


Figura 2.4: Desempeño mostrado por las tablas *hash* distribuidas Chord y Kademlia en (a) términos de confiabilidad y (b) costo de mantenimiento.

que el protocolo de autoorganización no es capaz de construir la topología lógica de anillo bajo la restricción de que existe rotación de los participantes desde la creación de la red P2P. Esto provoca que los nodos sólo puedan alcanzar a un subconjunto de participantes, afectándose directamente a la razón de búsquedas exitosas según lo explicado en el apartado 2.2.2. La segunda es que el protocolo de autoorganización en cuestión no considera las características estadísticas del tiempo de sesión de los participantes.

Explícitamente, el protocolo de autoorganización de Chord permite que los nodos nuevos se inserten en las listas de sucesores, pudiéndose sustituir así a aquellos participantes que tienen mayor probabilidad de permanencia y menor proporción [16, 54]. Esta problemática de Chord también se muestra en [53]. Como resultado de esto, es muy probable que el estado de los nodos sea incorrecto independientemente del tamaño de la lista de sucesores. Es por esto que la curva de desempeño obtenida de emplear una lista de sucesores de tamaño 8 es similar a la de 16 antes de los puntos de ruptura que ambas presentan (ver figura 2.4(a)).

Las razones por las que Kademlia exhibe un alto nivel de confiabilidad son las siguientes. La primera es que el tráfico de red contribuye al mantenimiento de la tabla *hash* distribuidas

dado que los nodos actualizan su estado cada vez que se lanza una búsqueda. El efecto de esto puede observarse en el nivel de confiabilidad de cada curva de desempeño de Kademia, donde la configuración  $\langle 3, 8, 600 \rangle$  muestra un mayor nivel de confiabilidad que la configuración restante (ver figura 2.4(a)). La segunda es que Kademia está diseñada para aprovechar el comportamiento estadístico de los nodos ya que las entradas de los contenedores no necesariamente se modifican con la entrada de nodos nuevos. Además, las entradas de los nodos que llevan un tiempo considerable en el sistema se conservan en los contenedores debido a que es muy probable que dichos nodos permanezcan por más tiempo. La tercera es que las reglas que forman la topología lógica de Kademia son más flexibles que las de Chord ya que resulta más complicado conectar a cada nodo con su sucesor que conectar a un nodo con cualquiera que cumpla con una longitud de prefijo dado.

Los resultados del costo de mantenimiento de Chord y Kademia se muestran en la figura 2.4(b), donde se puede notar que mantener la funcionalidad de Kademia es más caro cuando el nivel de rotación de los participantes aumenta, mientras que lo contrario ocurre con Chord. La tendencia exhibida por las curvas de desempeño de Kademia tiene su explicación en el hecho de que mientras mayor es el nivel de rotación de los participantes, mayor es el número de consultas que deben de enviarse para integrar a los nodos nuevos. En el caso de Chord, el número de mensajes de mantenimiento decrece porque no hay mucha oportunidad de generar mensajes de mantenimiento dado que los enlaces lógicos que integran la topología del anillo son incorrectos. Además es interesante notar que el costo de mantenimiento de Kademia es menor que el de Chord en el intervalo de rotación de los participantes comprendido entre 0.125 y 0.75 %churn/s. Esto se debe a que el tiempo entre llamadas a la rutina de estabilización de Chord se configura con un valor corto de cinco segundos, lo cual hace que los nodos envíen aproximadamente cuatro mensajes de control por segundo para actualizar su estado.

### 2.3.2. Evaluación con pares estables

En las figuras 2.5(a) y (b), se muestran los resultados obtenidos de evaluar Chord y Kademia bajo el escenario dos. Cada valor corresponde al promedio de 25 ejecuciones independientes. Con el fin de ilustrar la dinamicidad de la red, en el eje  $x$  de ambas subfiguras se indica la tasa de rotación normalizada promedio de cada una de las composiciones mostradas en la tabla 2.2.

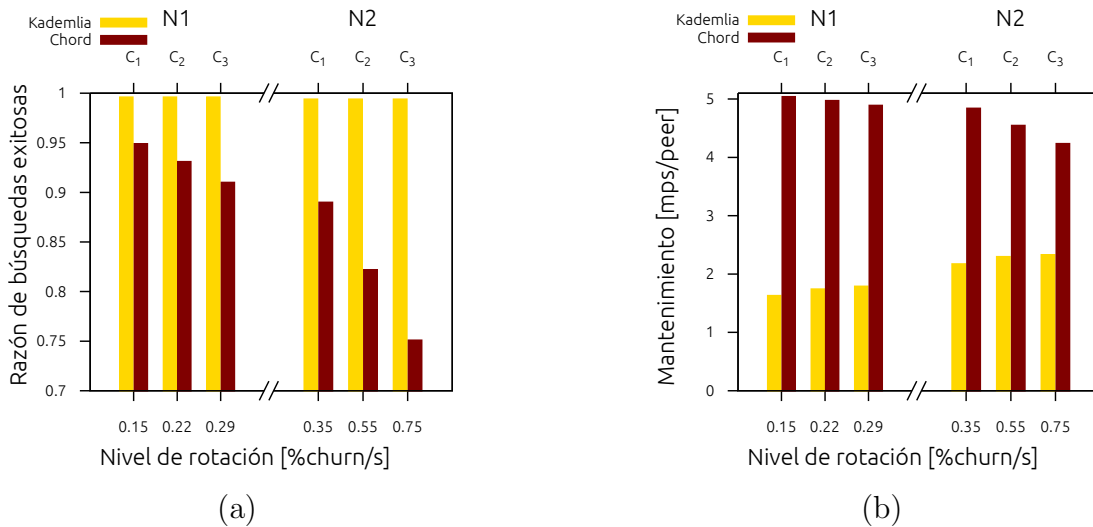


Figura 2.5: Desempeño mostrado por Chord y Kademia evaluados en una red con distintas composiciones de participantes. (a) Nivel de confiabilidad. (b) Costo de mantenimiento.

Como se observa en la figura 2.5(a), el nivel de confiabilidad de Chord decrece conforme aumenta el nivel de rotación de participantes. Esto reafirma los resultados descritos en el apartado anterior ya que Chord no obtiene beneficios de los benefactores porque los nodos no están obligados a mantenerlos en su lista de sucesores. Esto se nota inclusive en las barras que corresponden a la composición  $C_1$ , donde la red se integra por una fracción de 0.3 benefactores. En contraste, la figura 2.5(a) también muestra como el nivel de confiabilidad de la configuración  $\langle 1, 8, 600 \rangle$  de Kademia aumenta su confiabilidad aún más que la configuración  $\langle 3, 8, 600 \rangle$  mostrada en la figura 2.4(a). Es importante resaltar que la mejora de este aumento en el nivel de confiabilidad se da aun en las composiciones con un 10% de benefactores, las

cuales se denotan con la etiqueta  $C_1$ .

Al igual que en los resultados mostrados en el apartado pasado, la figura 2.5(b) muestra que el costo de configurar Chord con un intervalo de llamadas entre estabilizaciones de cinco segundos es muy elevado. De hecho, el costo del mantenimiento es cercano a los cinco mps/peer para el caso etiquetado como  $N_1, C_1$ . También, se puede notar que el mantenimiento de Chord decae conforme aumenta el nivel de rotación de los participantes, reafirmando así la relación entre el nivel de confiabilidad y el costo de mantenimiento descrita en el apartado anterior. En el caso de Kademlia, la figura 2.5(b) muestra que tal estructura requiere un costo de mantenimiento mucho menor que el que Chord necesita. Ahí, también es posible observar que el costo del mantenimiento de Kademlia aumenta conforme aumenta el nivel de rotación de los participantes, tal como se observa en los resultados descritos en el apartado anterior.

## 2.4. **Discusión**

Del análisis de los resultados obtenidos de evaluar el nivel de confiabilidad y el costo de mantenimiento de Chord y Kademlia se identifican las siguientes observaciones: (1) la funcionalidad de la red lógica depende de su establecimiento correcto, (2) la red lógica puede mantenerse correctamente aprovechando el tráfico de red y (3) el desempeño de las tablas *hash* distribuidas mejora si las características de la red subyacente se explotan. Estas observaciones son la base para el desarrollo de estrategias que soporten el mantenimiento de redes estructuradas para redes ad hoc móviles, tal como se enuncia a continuación.

El servicio de búsqueda provisto por las tablas *hash* distribuidas ve comprometido su funcionamiento si la red lógica no se establece correctamente, como se muestra con el caso de Chord. En la literatura, se han propuesto varias tablas *hash* distribuidas para redes ad hoc móviles [20, 22–27], sin embargo, todas ellas asumen que la topología lógica se establece exi-

tosamente bajo ciertas condiciones especiales y sin dar evidencia de ello. Específicamente, en [20, 22, 23, 25] se asume que la red lógica puede formarse a partir del proceso de unión de los nodos. En otras propuestas [24, 26, 27] se relaja el problema asumiendo que la red autoarranca a partir de un conjunto de nodos. Aunque el fenómeno que evita el establecimiento de la topología lógica de Chord no se presenta en las redes ad hoc móviles, existe la condición de que la topología física de la red no es estacionaria, por lo que no se puede asegurar que las tablas *hash* distribuidas se establecen correctamente a menos que su diseño incorpore un protocolo destinado a tal función.

El mantenimiento de la estructura de datos distribuida debe aprovechar el tráfico de red. Por ejemplo, se puede sacar provecho de la resolución de las consultas para actualizar el estado de los nodos que participen en el proceso, los cuales serán bastantes en una MANET ya que las comunicaciones son omnidireccionales y, como se explica en el siguiente capítulo, los nodos se aglomeran dentro de áreas populares. Dicha estrategia no es aprovechada por las tablas *hash* distribuidas para redes ad hoc móviles citadas hasta el momento.

En este punto, vale la pena mencionar que no todas las técnicas que mejoran el desempeño en las tablas *hash* distribuidas pueden pasar directo al ámbito de las redes ad hoc móviles, p. ej., enviar varias consultas para resolver una búsqueda puede no ser muy buena estrategia ya que un objetivo de emplear redes lógicas en este contexto es reducir la cantidad de mensajes de control para proveer un servicio. Inclusive, las ventajas de usar una topología lógica como la de Kademlia pueden no aparecer en el ámbito de las redes ad hoc móviles, como se muestran en [23, 25], donde se propone una topología lógica basada en un árbol binario completo. Para hacer las conexiones lógicas, se emplea un mecanismo determinista que asigna a los nodos un identificador que comparte similitud en prefijo con alguno de sus vecinos. Desafortunadamente, este mecanismo no asegura que el espacio de claves preservará su propiedad de unicidad porque nunca se comprueba que un identificador dado no esté ocupado

en la red. La probabilidad de que eso ocurra en el caso de Kademia es despreciable porque el identificador lógico se calcula con una función *hash* que exhibe una bajísima probabilidad de colisión porque los valores que regresa corresponden a  $2^{160}$  claves diferentes [13].

Finalmente, los resultados presentados en esta evaluación indican que el desempeño de las tablas *hash* distribuidas se ve mejorado cuando se explotan las características estadísticas de la infraestructura subyacente. En efecto, el hecho de que los nodos que ejecutan Kademia mantengan en su estado las entradas que corresponden a los que tienen alta probabilidad de permanecer en línea hace posible que el servicio de búsqueda exhiba una confiabilidad cercana al 100%. Esto bajo el supuesto de que el 10% del total de participantes exhibe tiempos de vida largos, como se muestra en el apartado 2.3.2. Mecanismos como los usados por Kademia pueden diseñarse si se conocen las cualidades de las redes ad hoc móviles. Por ello, en el siguiente capítulo se presenta un análisis de características estadísticas de redes ad hoc móviles donde los nodos se mueven siguiendo patrones de movilidad humana.





# Capítulo 3

## Análisis experimental de características topológicas de las MANET

El reto más grande que los protocolos de redes ad hoc móviles enfrentan es que el movimiento de los nodos hace que la topología de la red sea dinámica. De hecho, en [36–38] muestran que el desempeño exhibido por estos protocolos depende en gran medida de la manera en que la topología de la red cambia. Por esta razón, estos protocolos deberían ser evaluados usando el modelo que mejor represente el movimiento de las entidades que las conforman. Para establecer una red P2P sobre una MANET, es necesario conocer si la conectividad presenta variaciones abruptas, ya que de ser así se limitaría el tipo de técnica de búsqueda que se puede emplear.

En las investigaciones relacionadas con redes ad hoc móviles frecuentemente se asume que son humanos los que portan los dispositivos móviles y por algo más de dos décadas se han presentado distintos modelos, varios de ellos descritos en [55–57], que buscan representar el

movimiento humano. Modelar este factor con los elementos necesarios para representar detalladamente la movilidad humana permite observar el estado que puede exhibir la conectividad de las redes ad hoc móviles en escenarios cercanos a la realidad.

Por la razón mencionada anteriormente, en esta investigación se analizan las características de la topología de las redes ad hoc móviles en un escenario donde los nodos se mueven bajo el modelo SLAW, el cual representa las propiedades de la movilidad humana descritas en [32–35]. Este objetivo se define por la necesidad de identificar el tipo de búsqueda que mejor se adapte a las redes ad hoc móviles.

Para alcanzar esta meta, se realiza una revisión de la literatura que describe el contexto en el que se encuentra el estudio sobre las características de la topología de las redes ad hoc móviles bajo diferentes condiciones de movilidad (sección 3.1). Enseguida, en la sección 3.2 se define un marco de evaluación que permite observar la conectividad de la red y el tiempo de vida de las rutas generadas por un protocolo de encaminamiento para redes ad hoc móviles. Después, se analizan los resultados obtenidos del marco de evaluación antes mencionado; dicho análisis se presenta en la sección 3.3. Finalmente, una discusión sobre los resultados obtenidos se presenta en la sección 3.4. A partir del contenido de este capítulo, se realizó un artículo publicado en [39].

### 3.1. Revisión de la literatura

En este apartado se explica el modelo de movilidad de selección aleatoria de punto de recorrido (*random waypoint*, RWP) y el modelo de caminata de menor acción autosimilar (*self-similar least-action walk model*, SLAW). Después, se ilustra brevemente el funcionamiento del protocolo de encaminamiento AODV (*ad hoc ondemand distance vector*) para finalmente describir los trabajos [58] y [59] que muestran el tiempo de vida de ruta característico del modelo

RWP.

### 3.1.1. Modelos de movilidad

Se define como *modelo de movilidad* al conjunto de reglas que determinan el movimiento de los nodos dentro de cierta área. Un modelo de movilidad captura las características relevantes que describen el movimiento de los nodos tales como velocidad, aceleración, tiempo de pausa y ubicación a lo largo del tiempo. Modelos de movilidad más complejos también consideran otros elementos tales como restricciones físicas y movimiento en grupo.

Los modelos de movilidad que recientemente han sido publicados [60–62] son el resultado de un largo proceso evolutivo durante el cual diversas características del fenómeno de la movilidad humana se han ido agregando o afinando gradualmente. Cada modelo nuevo mejora a uno anterior integrando conocimiento más preciso sobre la movilidad humana. Una descripción resumida de varios modelos de movilidad se encuentra descrita en [55–57].

En este capítulo únicamente se describen dos productos que se encuentran en extremos contrarios del proceso evolutivo experimentado por los modelos de movilidad: el modelo de movilidad de selección aleatoria de punto de recorrido (*random waypoint*, RWP) y SLAW.

Descrito en [63], el modelo RWP se caracteriza por ser muy popular para evaluar redes ad hoc móviles [57], además las reglas que lo componen son simples [64] y requiere relativamente pocos recursos computacionales para ser ejecutado. Dada su popularidad, este modelo ha sido analizado para entender las condiciones en las que se alcanza su estado estable con el fin de obtener resultados de simulación confiables [65, 66].

El modelo RWP funciona de la siguiente manera. Al comienzo, a los nodos se les asigna un punto inicial dentro de un área de simulación previamente definida. Después, los nodos

permanecen en dicho punto durante  $t$  segundos, donde el valor de  $t$  es seleccionado aleatoriamente del intervalo  $[pause_{\min}, pause_{\max}]$ . Enseguida de la pausa, a lo nodos se les asigna un nuevo destino dentro del área de simulación al cual se dirigen siguiendo una trayectoria rectilínea a velocidad constante. El valor de dicha velocidad se elige de manera aleatoria del intervalo  $[speed_{\min}, speed_{\max}]$ , donde  $speed_{\min} > 0$ . Una vez alcanzado el punto destino, los nodos hacen de nuevo una pausa para después continuar con el proceso de movilidad de manera cíclica.

En un punto evolutivo más avanzado se tiene al modelo SLAW, el cual integra varios descubrimientos recientes sobre la movilidad humana, los cuales se describen a continuación:

1. Áreas de movilidad confinadas [33]. Esta característica representa el hecho de que la gente se mueve en mayor medida dentro de áreas confinadas. De hecho, las personas pueden tener áreas de movilidad completamente diferentes.
2. La distribución espacial de los puntos de recorrido (*waypoint*) visitados por los humanos pueden ser modelados por puntos distribuidos de manera autosimilar. Con esta distribución se modela el hecho de que la gente es atraída hacia áreas consideradas populares, lo que crea un fenómeno de agrupamiento que puede ser observado a diferentes escalas [32].
3. La gente tiende a visitar los destinos más próximos a su punto de recorrido actual cuando tienen que ir a varios lugares en un único viaje [32].
4. Tanto el tiempo de pausa como la longitud de los desplazamientos entre dos puntos de recorrido presentan características estadísticas que se ajustan bien con una distribución de cola pesada [34].
5. El tiempo entre contactos, es decir, el tiempo que pasa entre dos encuentros de un mismo par de personas se modela bien con una distribución de cola pesada [35].

Para cumplir con la primera propiedad, un conjunto de puntos de recorrido  $W$  se distribuye sobre un área dada. Estos puntos se agrupan para formar áreas confinadas  $c_i$  de radio  $r$ , medido en metros, donde el subíndice  $i$  denota el número de área confinada. A cada nodo  $k$  se le asignan distintas áreas confinadas para modelar el hecho de que las personas pueden tener áreas de movilidad distintas. Además, esta estrategia fuerza a los nodos a moverse mayormente dentro de las áreas que les fueron asignadas.

La segunda propiedad se modela distribuyendo los puntos de recorrido de manera autosimilar. El nivel de autosimilitud se controla por el parámetro de Hurst  $H$ , donde  $0.5 < H < 1$ . Consecuentemente, el número cardinal de cada área confinada no será uniforme, sino que existirán pocas áreas con un número considerable de puntos de recorrido y otras con unos pocos. El modelo SLAW elige las áreas confinadas de cada nodo con base en su número cardinal, siendo aquellas con un número grande de elementos las más probables de ser asignadas. Esto resulta en áreas que con mucha probabilidad estarán aglomeradas por un número considerable de nodos.

Para representar la tercera característica, en el modelo SLAW se hace lo siguiente. Después de que los nodos tienen asignado un conjunto  $C_k$  de áreas confinadas,  $c_i$ , se les asigna un punto de partida y un viaje. El primero es elegido de manera aleatoria del conjunto  $C_k$ . El segundo se compone de entre 120 y 150 puntos de recorrido tomados de  $|C_k| - 1$  áreas confinadas de  $C_k$  y de un área confinada seleccionada aleatoriamente. El número de puntos de recorrido del área que no pertenece a  $C_k$  es de entre cinco y diez por ciento de su número cardinal. Después, los nodos hacen sus viajes eligiendo su próximo destino mediante el algoritmo de planeación de recorrido de menor acción (*least-action trip planning*, LATP). El algoritmo determina el siguiente punto de recorrido que un nodo va a visitar tomando como referencia la distancia que hay entre la ubicación actual del nodo y los destinos que no ha visitado. La selección del siguiente destino depende del valor que se le dé a un parámetro  $a$ . Si  $a = 0$ , entonces la

selección es uniformemente aleatoria, pero se recomienda un valor de  $a$  entre uno y tres para representar el hecho de que los humanos buscan reducir las distancias que recorren.

La cuarta característica se modela haciendo que los nodos que alcanzan cierto punto de recorrido permanezcan en éste durante un tiempo de pausa, que a diferencia de RWP, es muestreado de una distribución de Pareto truncada. Ya que los puntos de recorrido se encuentran distribuidos de manera autosimilar, basta con que los nodos hagan su viaje para que exhiban desplazamientos con distribución de cola pesada. Bajo el modelo SLAW los viajes tienen una duración preestablecida de doce horas.

La última característica es consecuencia directa del cómo los nodos se mueven en un área donde los puntos de recorrido están distribuidos de manera autosimilar, del movimiento dentro de áreas confinadas y de la aglomeración en áreas populares. En conjunto, esto hace que los nodos se encuentren frecuentemente dentro de las áreas populares y que, una vez fuera de ellas, pase bastante tiempo para que vuelvan a encontrarse.

### 3.1.2. Protocolo de encaminamiento AODV

Un *protocolo de encaminamiento* se compone por reglas de comunicación ejecutadas de manera distribuida para determinar la secuencia ordenada de nodos que permitiría el flujo de paquetes de datos enviados desde un emisor hacia un destino. A dicha secuencia se le conoce como *ruta*.

En la literatura se han presentado un gran número de protocolos de encaminamiento para redes ad hoc móviles que pueden clasificarse de acuerdo con la estrategia de descubrimiento que emplean [67], es decir, en reactivos y proactivos:

- Protocolos reactivos. Siguen la estrategia de establecer rutas bajo la demanda por

medio de algún tipo protocolo de inundación. Además, pueden adaptarse a las rutas a los cambios topológicos de la red mediante el intercambio de mensajes de control. Estos protocolos presentan la ventaja de utilizar el canal de comunicaciones únicamente cuando las aplicaciones lo requieren, pero tienen la desventaja de tardar cierto tiempo en descubrir nodos destino. Además, pueden entorpecer su funcionamiento y el de otros protocolos durante el proceso de establecimiento de ruta, en especial cuando el número de nodos de la red excede ciertos límites.

- Protocolos proactivos. Estos protocolos intentan recolectar tanta información sobre la topología de la red como sea posible a través del intercambio programado de mensajes entre nodos. Siguiendo la estrategia proactiva, la ruta entre un emisor y cualquier receptor está determinada aunque no sea previamente solicitada. La ventaja de estos protocolos es que el establecimiento de las comunicaciones exhibe baja latencia. La desventaja es que requieren del uso del canal de comunicaciones aunque las aplicaciones no generen tráfico de red. Además, requieren que los nodos intercambien con mayor frecuencia su información topológica cuando la conectividad de la MANET cambia abruptamente.

Este trabajo explora el desempeño del protocolo reactivo denominado AODV [68], debido a que ha sido usado como referencia para contrastar el desempeño de protocolos reactivos. AODV está diseñado para no depender específicamente de las características del medio físico empleado para transmitir datos, por lo que puede ser ejecutado en redes cableadas e inalámbricas. El protocolo AODV requiere para operar que los enlaces inalámbricos sean bidireccionales y que los nodos puedan recibir las difusiones (*broadcast*) de sus vecinos locales. En resumen, a continuación se explica su funcionamiento con base en las dos operaciones principales que lleva a cabo: el descubrimiento de ruta y la detección de rutas inválidas.

Suponiendo que los nodos conocen a sus vecinos a un salto, el procedimiento de descubri-

miento de ruta comienza cuando un emisor difunde un mensaje RREQ de solicitud de ruta a sus vecinos. Los nodos que reciben este mensaje lo reenvían si es que no tienen una ruta hacia el destino solicitado, de lo contrario difunden un mensaje de respuesta RREP. Así, mediante este protocolo de inundación, el mensaje RREQ llega al destino o a un nodo que conoce cómo alcanzarlo. Durante el proceso de inundación, los nodos intermedios entre el emisor y el destino registran la identidad del vecino del cual recibieron la primera copia del mensaje RREQ para establecer la *ruta de reversa* por la que el mensaje RREP llegará al emisor. Una vez que un nodo puede responder la solicitud de ruta, envía el mensaje de respuesta RREP al emisor usando la ruta de reversa. Durante este proceso, los nodos intermedios establecen una *ruta de ida* marcando la identidad del nodo del que recibieron el mensaje RREP. Cuando el mensaje RREP llega al emisor del RREQ, se da por finalizado el proceso de descubrimiento de ruta.

Debido a la movilidad de los nodos, las rutas establecidas por el protocolo AODV pueden invalidarse porque los nodos que la integran dejan de mantener su conectividad original. Este evento puede detectarse de manera reactiva o proactiva. La estrategia reactiva consiste en esperar a que un paquete no pueda ser enviado al siguiente salto. Al seguir la estrategia proactiva, los nodos que integran una ruta intercambian mensajes para detectar enlaces locales fallidos. Así, los nodos intermedios pueden notificar más rápidamente a los emisores que la ruta hacia el destino es inválida.

La versión de AODV descrita en [68] presenta algunos inconvenientes que han sido mejorados en la versión publicada en el RFC 3561 [69]. La primera de ellas reduce el costo del descubrimiento de ruta, ya que en lugar de emplear la estrategia de inundación se utiliza la de búsqueda por anillo expansivo (*expanding ring search*). Bajo esta estrategia, el proceso de descubrimiento de ruta se va haciendo gradualmente: primero se contactan a todos los vecinos alcanzables a unos cuantos saltos. Si el procedimiento falla, entonces el mensaje



RREQ se envía a nodos que se encuentran más allá del área explorada. La segunda mejora es un procedimiento de recuperación de ruta que repara los enlaces inválidos mediante búsqueda por anillo expansivo. Durante este procedimiento, el nodo intermedio debe almacenar el paquete dirigido hacia el destino. Si el procedimiento de reparación de ruta es exitoso, entonces el emisor puede continuar con la transferencia de paquetes sin la necesidad de ejecutar nuevamente el proceso de descubrimiento de ruta.

### 3.1.3. Trabajo relacionado

A continuación, se describen los trabajos [58] y [59], donde se reportan los efectos que la movilidad causa al tiempo de vida de las rutas, el cual influye directamente en el tiempo de vida de los enlaces lógicos.

En [58], se examinan las características estadísticas de la duración de los enlaces inalámbricos y de las rutas generadas por los protocolos de encaminamiento reactivo AODV y DSR [70] (*dynamic source routing*), bajo los modelos de movilidad RWP, RPGM (*reference point group mobility*), *Freeway* y *Manhattan*. Este trabajo muestra que el tiempo de vida de ruta puede modelarse con una distribución exponencial cuando los nodos se mueven a una velocidad moderada o alta ( $V_{max} \geq 10$  m/s) y la longitud de la ruta es mayor o igual que dos saltos. Bajo esas condiciones, los autores reportan que la duración promedio del tiempo de vida de las rutas es menor que 20 s.

Un modelo analítico diseñado para predecir el tiempo de vida de las rutas de longitud  $d$  a una velocidad de 1 m/s se presenta en [59]. Usando el modelo RWP, en este trabajo se reporta que el tiempo de vida de las rutas disminuye conforme aumenta el número de nodos intermedios que la componen. Bajo estas circunstancias, el tiempo de vida más largo se observa en rutas de tres saltos, cuyo valor es menor que un minuto.

En estos trabajos se analiza el tiempo de vida de ruta bajo distintos modelos de movilidad e intervalos de velocidad. Con base en los resultados ahí reportados, es posible intuir que construir y mantener una red lógica sobre una MANET puede ser una estrategia poco eficiente ya que las rutas sobre las que se establecen enlaces lógicos duran muy poco ya que la topología física no conserva su misma conectividad por mucho tiempo. No obstante, en los escenarios considerados en investigaciones previas se emplean modelos que no representan ninguna característica estadística de la movilidad humana, por lo que no es posible descartar que una red lógica pueda ser establecida exitosamente en una MANET. Por lo tanto, es necesario determinar las características estadísticas de las redes ad hoc móviles, considerando el hecho de que son humanos los que portan los dispositivos que las integran para así determinar la viabilidad de emplear redes lógicas para ofrecer servicios de búsqueda.

## 3.2. Metodología experimental

En este capítulo se presenta el marco de evaluación diseñado para obtener las características estadísticas de la topología de las redes ad hoc móviles bajo los modelos de movilidad RWP y SLAW. Además, se presenta el procedimiento llevado a cabo para medir el tiempo de vida de las rutas multisalto generadas por el protocolo AODV.

Dado que cada modelo de movilidad produce diferencias en la distribución espacial de los nodos, el primer paso de la metodología es determinar las propiedades de la conectividad que resultan de usar distintos modelos de movilidad. Para ello, mediante simulación se observa cuántos nodos son *alcanzables* a  $d$  saltos. Por definición, se dice que un nodo  $x$  es alcanzable por otro  $y$  si existe una secuencia de nodos adyacentes que inicia en  $x$  y termina en  $y$  o, sencillamente, si existe una ruta entre  $x$  y  $y$ . Para realizar este paso, se consideran varios escenarios con distintas combinaciones de modelo de movilidad y tamaño de red.

Como segundo paso, se observa el desempeño de las rutas multisalto formadas por el protocolo AODV bajo distintos tamaños de red. En este experimento, todos los nodos generan una consulta cada  $t$  segundos, donde el valor de  $t$  es muestreado de una distribución normal para agregar aleatoriedad al proceso. Las consultas son enviadas a destinos seleccionados al azar que se encuentran a una distancia de  $d$  saltos del origen, donde  $d$  es un parámetro configurable. Los emisores, después del establecimiento de ruta, envían una consulta que los destinos responden inmediatamente después de recibirla. Si el emisor recibe el mensaje de respuesta dentro de *timeout* segundos, entonces la búsqueda se considera exitosa. Cuando es momento de generar otra consulta, el emisor verifica si la anterior fue o no exitosa. De haber sido exitosa, el emisor envía una nueva consulta al mismo destino anteriormente contactado. De otra manera, el emisor selecciona aleatoriamente otro destino también localizado a  $d$  saltos. Debido a la movilidad, es posible que en un instante dado el emisor no tenga vecinos a  $d$  saltos. Bajo esta condición, los emisores intentan contactar nuevamente a algún nodo a  $d$  saltos  $t$  segundos después de la consulta fallida.

### 3.2.1. Medidas de desempeño

Con el fin de cuantificar las características de la topología de la red, se emplean las siguientes medidas:

- Razón de conectividad. Como recordatorio, en el primer paso de la metodología se observa si los nodos tienen vecinos a  $d$  saltos, lo cual puede resultar en cierto o falso. Siendo así, la razón de conectividad  $C_r$  es el número de veces  $c_t$  que es posible alcanzar a un nodo a  $d$  saltos entre el número de veces  $T$  que la observación es hecha. Esta medida puede ser usada para determinar la probabilidad de alcanzar a un nodo en función de

su distancia. Se calcula con la fórmula:

$$C_r = c_{\text{times}}/T \quad (3.1)$$

- Razón de aislamiento. Esta medida es el número de veces  $a_t$  que los nodos se encuentran sin vecinos locales entre el número de veces  $T$  en que los vecindarios se observan. Esta medida es complemento de la razón de conectividad cuando  $d = 1$ . La medida permite estimar la probabilidad de que un nodo esté aislado bajo cierto modelo de movilidad. La fórmula para calcularla es:

$$A_r = a_{\text{times}}/T \quad (3.2)$$

- Número de vecinos promedio. Como el nombre indica, la medida es el promedio de vecinos que un nodo tiene a  $d$  saltos. La medida complementa la información provista por la razón de conectividad.

El desempeño de las rutas formadas por el protocolo AODV se determina usando estas medidas:

- Razón de búsquedas exitosas. Denotada por  $L_r$ , es el número de consultas respondidas  $q_{\text{success}}$  dividido por el número total de enviadas  $Q$ . Esta medida determina el número de veces que un protocolo de encaminamiento puede establecer exitosamente una ruta entre dos terminales que son alcanzables al momento en que el descubrimiento es solicitado. Su fórmula es:

$$L_r = q_{\text{success}}/Q \quad (3.3)$$

- Tiempo de ida y vuelta (*round-trip time*, RTT). Es el intervalo de tiempo medido a partir del instante  $t_{\text{sent}}$  en que una consulta es enviada hasta el instante  $t_{\text{recv}}$  en que

la respuesta se recibe. La medida es útil para determinar el retardo de comunicación debido a las condiciones de red cuando se establece un enlace lógico entre un par de nodos. Se calcula con la fórmula:

$$\text{RTT} = t_{\text{recv}} - t_{\text{sent}} \quad (3.4)$$

- Tiempo de vida de ruta. La medida  $T_{\text{route}}$  es la duración de una ruta multisalto entre una pareja de nodos, es decir, el tiempo que transcurre desde su establecimiento  $t_{\text{init}}$  hasta el de su rompimiento  $t_{\text{break}}$ . Además, determina los efectos que la movilidad produce sobre un protocolo de encaminamiento ya que un valor pequeño indica que los nodos se desplazan abruptamente sobre el área de simulación. La siguiente fórmula permite su cálculo:

$$L_{\text{route}} = t_{\text{break}} - t_{\text{init}} \quad (3.5)$$

### 3.2.2. Configuración de la simulación

Los experimentos descritos arriba se realizan mediante simulaciones de eventos discretos. El escenario de simulación que se considera es un área cuadrada de  $1000 \times 1000 \text{ m}^2$  que representa abstractamente un campus universitario. Dentro de esta área, los nodos se mueven conforme a los modelos SLAW y RWP.

La configuración del modelo SLAW es la siguiente. El número cardinal del conjunto de puntos de recorrido, denotado por  $|W|$ , se fija en 2000. El grado de autosimilitud controlado por el parámetro  $H$  se fija en 0.75. El radio del agrupamiento que determina el tamaño máximo de las áreas confinadas es de 40 m. La longitud del radio determina el área de edificios de un campus universitario. El parámetro  $a$  se fija en 3 para representar recorridos bien planeados. El tiempo de pausa se modela con una distribución de Pareto truncada, con parámetro

de forma  $\alpha = 1.36$ , valor mínimo de 30 s y máximo de 9054 s. Estos valores se toman de [34], donde reportan la distribución del tiempo de pausa que corresponde a un campus universitario. La función de distribución de la probabilidad resultante para el tiempo de pausa es  $138.8699/x^{2.36}$ . A diferencia del modelo original de SLAW, en esta implementación los recorridos no tienen una duración fija de 12 horas sino más bien arbitraria que depende del tiempo que tarde un nodo en terminar su viaje. En la figura 3.1(a), se muestra un ejemplo del viaje recorrido por un nodo bajo la configuración ya descrita.

En el artículo donde se describe SLAW se recomienda emplear el modelo de velocidad presentado en [34], el cual representa tanto la velocidad de vehículos como de peatones. Dado que en estos experimentos se asume que el campus se recorre sólo a pie, aquí se emplea el modelo de velocidad peatonal propuesto en [71] en lugar del descrito en [34]. Bajo el primero, la velocidad se toma de una distribución normal con media  $\mu = 1.36$  m/s y varianza  $\sigma^2 = 0.0361$  m<sup>2</sup>/s<sup>2</sup>.

El modelo RWP se configura de la siguiente manera. Con base en [66], la velocidad y el tiempo de pausa se muestrean de una distribución uniforme  $\mathcal{U}_v(0.1, 20)$  m/s para la velocidad y de  $\mathcal{U}_p(0, 20)$  s para el tiempo de pausa. Ya que los parámetros de configuración de RWP se determinan para probar el funcionamiento de un protocolo y rara vez tomando en cuenta las características del movimiento de entidades reales, para fines de comparación se modela la velocidad y el tiempo de pausa con respecto a las características de la movilidad humana. Así, se establece una configuración del modelo RWP nombrada movilidad humana de selección aleatoria de punto de recorrido (*human random waypoint*, HRWP). Para esta configuración, se considera el modelo velocidad normal presentado en [71] y el modelo del tiempo de pausa descrito [34], ambos con la configuración empleada en el modelo SLAW. En la figura 3.1(b), se muestra un recorrido realizado por un nodo siguiendo el modelo RWP.

Finalmente, la configuración de las terminales inalámbricas se establece de la siguiente for-

ma. Al modelo de los nodos se le asigna un componente que representa una tarjeta de red inalámbrica que ejecuta una implementación del protocolo IEEE 802.11g. La tarjeta de red simulada es ajustada con un parámetro de sensibilidad de -61 dBm para limitar el área de comunicación de los nodos a 50 m a la redonda. También se generan errores de transmisión mediante el modelo de error NIST [72]. En la capa de red, los nodos ejecutaban una implementación del protocolo AODV, conocida como AODVUU [73], desarrollada por la Universidad de Upsala. En la capa de aplicación, los nodos ejecutaron una aplicación UDP (*user datagram protocol*) que genera búsquedas por nodos alcanzables cada  $t$  segundos, donde  $t$  es una variable aleatoria Gaussiana con parámetros  $\mu = 60$  s y  $\sigma^2 = 36$  s<sup>2</sup>. Las búsquedas son fallidas si no se recibe respuesta del destino en un tiempo *timeout* menor a 20 s. En estos experimentos, los nodos no generan transferencias de archivos y sólo se consideran rutas no mayores a 6 saltos ya que en [74, 75] se menciona que el desempeño presentado por rutas multisalto largas es bajo, lo que las hace inutilizables para fines prácticos. El tamaño de cada consulta es de 512 bytes. Las características de la topología se observan cada 60 s.

Las configuraciones anteriores se implementaron en el simulador INET 2.5 [42] basado en el

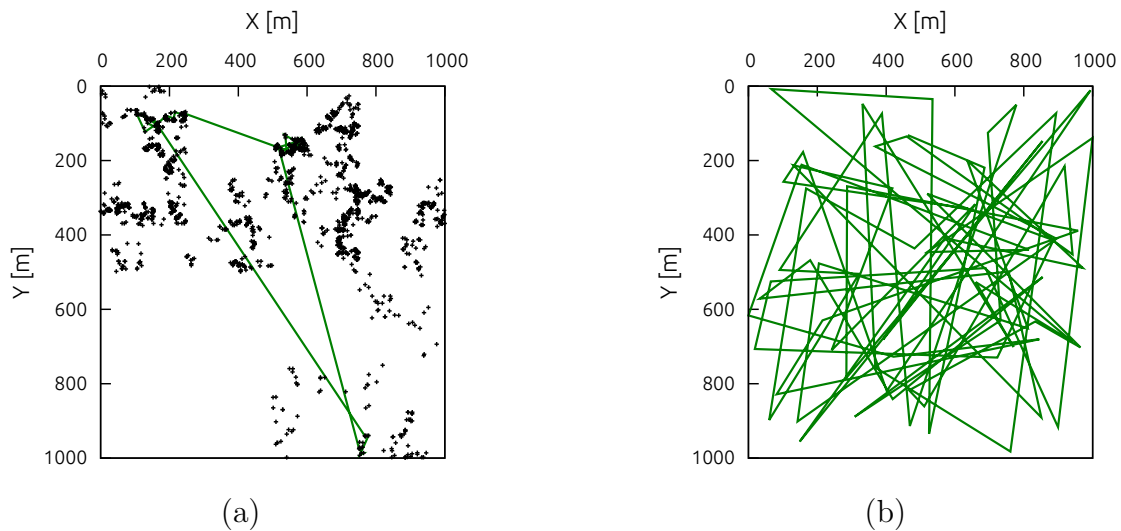


Figura 3.1: Muestras de un viaje recorrido por un nodo bajo (a) el modelo SLAW y (b) el modelo RWP.

marco de desarrollo de simulaciones OMNeT++ versión 4.6 [43]. Utilizando estas herramientas, los experimentos se ejecutan en dos etapas: una de calentamiento y una de mediciones. La primera se emplea para permitir que el modelo de movilidad alcance su estado estable, es decir, que la posición actual de los nodos no dependa de su posición inicial. Para ello, se observa cuánto tiempo un nodo tarda en completar un viaje en el peor de los casos. No obstante, un criterio más certero es observar la invariabilidad de la distribución espacial de los nodos, de manera similar a como se hace en [76]. La segunda tiene por objetivo la obtención de datos para calcular las medidas de desempeño. La duración de la primera fase es de diez horas y la de la segunda de 72 horas, ambas horas de simulación.

### 3.3. Resultados

En esta sección, se explican los resultados obtenidos de los experimentos descritos en el apartado anterior. En la mayoría de los casos sólo se consideran los resultados obtenidos de los escenarios con tamaño de red de 25, 100 y 300 nodos ya que los resultados restantes no proveen conocimiento adicional.

#### 3.3.1. Análisis de la topología de red

Los resultados obtenidos de observar la razón de conectividad determinan la probabilidad de establecer rutas multisalto en una MANET bajo los modelos de movilidad RWP y SLAW. En la figura 3.2(a), se muestran los resultados correspondientes al escenario donde el tamaño de red fue de 25 nodos. En la figura claramente se puede apreciar que la razón de conectividad más alta se obtiene cuando los nodos siguen el modelo SLAW. Además, la figura muestra que las configuraciones RWP y HRWP exhiben una razón de conectividad similar a pesar de que



la configuración HRWP es calibrada con los mismos modelos de velocidad y tiempo de pausa usados para el modelo SLAW. Por ello, se puede deducir que el alto grado de conectividad que la topología presenta bajo el modelo SLAW se debe a la forma que los nodos siguen para desplazarse y no a qué tan rápido se mueven y qué tanto tiempo permanecen en pausa. Concretamente, es el movimiento dentro de las áreas confinadas y el algoritmo LATP lo que causa esta característica ya que obliga a los nodos a no desplazarse largas distancias y a permanecer en una misma región durante un tiempo considerable. En adición, la figura muestra que la probabilidad de tener vecinos a dos saltos bajo RWP y HRWP es cercana a cero. En contraste, la misma probabilidad tiene un valor cercano a 0.3 para el modelo SLAW.

Como es de esperarse, mientras el tamaño de la red se incrementa la conectividad mejora independientemente del modelo empleado. Precisamente, esto se observa en las figuras 3.2(b) y 3.2(c) donde se muestra el incremento en la razón de la conectividad para redes de tamaño 100 y 300, respectivamente. En la figura 3.2(b), se muestra que la razón de conectividad que presentan las configuraciones RWP y HRWP para rutas de un salto es cercana a 0.6, sin embargo, ésta decrece tan rápidamente que la probabilidad de encontrar vecinos a dos saltos es menor que 0.3. Esto no ocurre con el modelo SLAW ya que la probabilidad de alcanzar vecinos a tres saltos es poco menor que 0.5.

En la figura 3.2(c), se resalta aún más que el tamaño de la red mejora la razón de conectividad. Es interesante notar a través de la figura que la razón de conectividad de las configuraciones RWP y HRWP es mayor que la de SLAW a seis saltos. Esto se debe a que bajo SLAW los nodos son forzados a moverse dentro de las áreas confinadas, por lo que mientras más nodos se incluyan en la simulación, la densidad de nodos dentro de las áreas confinadas se incrementa, lo que hace más probable que los nodos alcancen a sus vecinos localizados a unos cuantos saltos, pero no hace fácil que los nodos de áreas confinadas distantes sean alcanzables. En contraste, las configuraciones RWP y HRWP teóricamente permiten la creación de rutas de

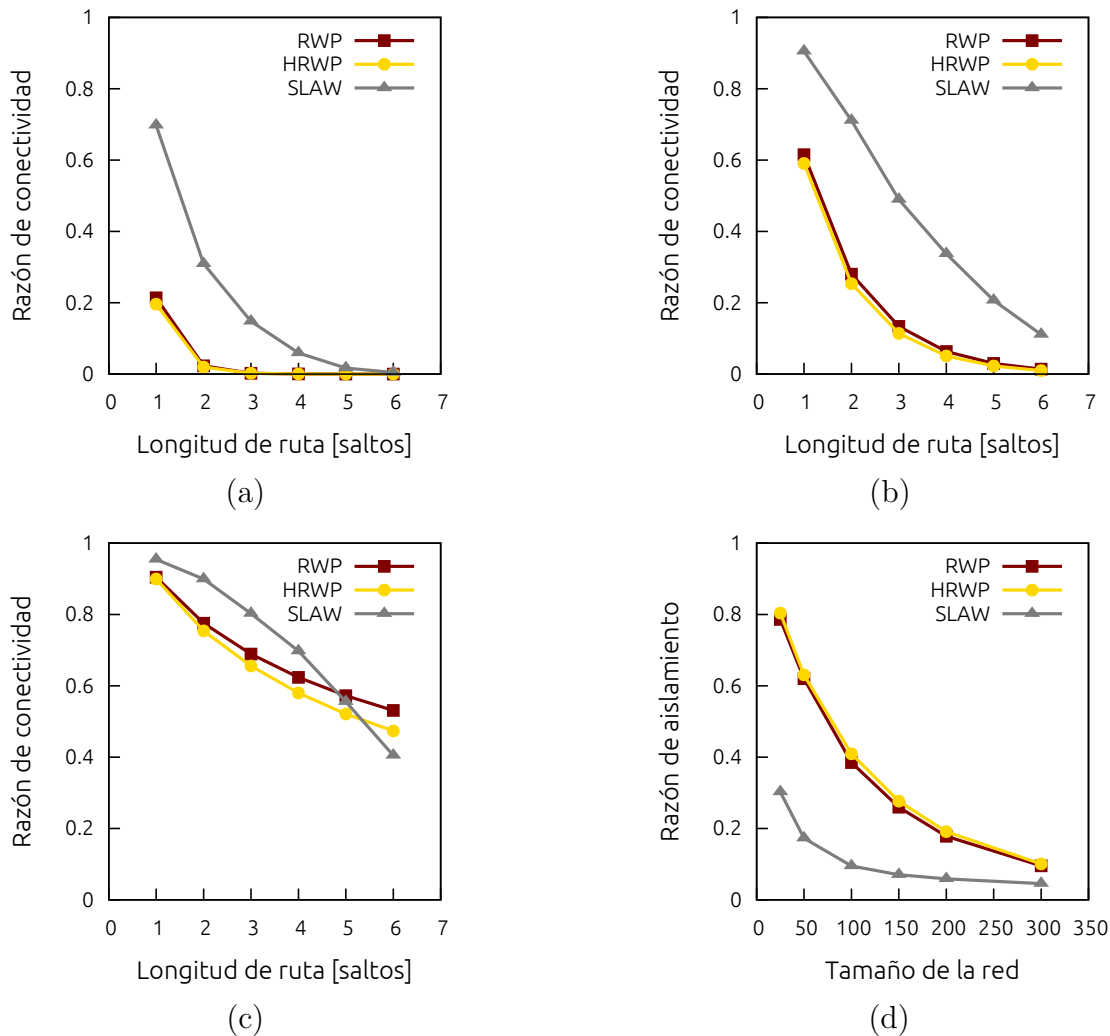


Figura 3.2: Razón de conectividad mostrada por los modelos de movilidad RWP y SLAW en redes de (a) 25, (b) 100 y (c) 300 nodos. En (d) se muestra la razón de aislamiento.

longitud de 28 saltos, si la ruta conecta a dos terminales ubicadas en las esquinas contrarias del área de simulación, que en este caso es de  $1000 \times 1000 \text{ m}^2$  y la distancia entre las terminales que forma la ruta es de 50 m aproximadamente.

Además, de la razón de conectividad se midió la razón de aislamiento, la cual se presenta en la figura 3.2(d). En ella, es posible observar que los nodos que se mueven de acuerdo con el modelo SLAW exhiben la razón de aislamiento más baja a distintos tamaños de red. Este desempeño se presenta inclusive en redes de 25 nodos, donde la razón de aislamiento es

aproximadamente de 0.3. El mismo rendimiento se alcanza con las configuraciones RWP y HRWP hasta que el tamaño de la red es de 150 nodos.

Para completar la información anterior, se mide el número promedio de vecinos que los nodos tienen a  $d$  saltos. Los valores promedio mostrados en la figura 3.3 incluyen intervalos con un nivel de confianza del 95 %. En la figura 3.3(a), se muestran las mediciones que fueron obtenidas al observar una red de 25 nodos. Sin importar el modelo de movilidad, la tendencia mostrada en la figura es que el número de vecinos decrece al aumentar el número de saltos. Además, en ella se puede notar claramente que los nodos tienen en promedio un vecino a una distancia no mayor que cinco saltos en los escenarios configurados con RWP y HRWP. Esto significa que las rutas multisalto no pueden ser fácilmente reparadas bajo dichas configuraciones por la carencia de nodos intermedios. En el caso del modelo SLAW, se presenta una ligera mejora ya que los nodos tienen en promedio dos vecinos locales.

Al igual que la razón de conectividad, el número de vecinos crece al aumentar el tamaño de la red. El resultado obtenido de observar una red de 100 nodos se ilustra en la figura 3.3(b). Ahí es posible notar que el número de vecinos permanece casi constante para las configuraciones RWP y HRWP. En el caso de SLAW, el número de vecinos locales crece en un factor aproximado de tres con respecto al escenario con 25 nodos, lo cual concuerda con la razón de conectividad mostrada en la figura 3.2. Además, la figura 3.3(b) muestra que los nodos pueden tener en promedio 2.5 vecinos a seis saltos con el modelo de movilidad SLAW con una probabilidad de 0.11 de acuerdo con los resultados mostrados en la figura 3.2(b). Bajo las configuraciones del modelo RWP, los nodos tienen en promedio 1.5 vecinos a seis saltos con una probabilidad de conectividad de 0.013. Este resultado es un orden de magnitud menor que la razón de conectividad observada con el modelo SLAW.

En los escenarios donde se fija un tamaño de red de 300 nodos, el número de vecinos alcanzables tiende a aumentar bajo las configuraciones RWP y HRWP (figura 3.3(c)). Este fenómeno

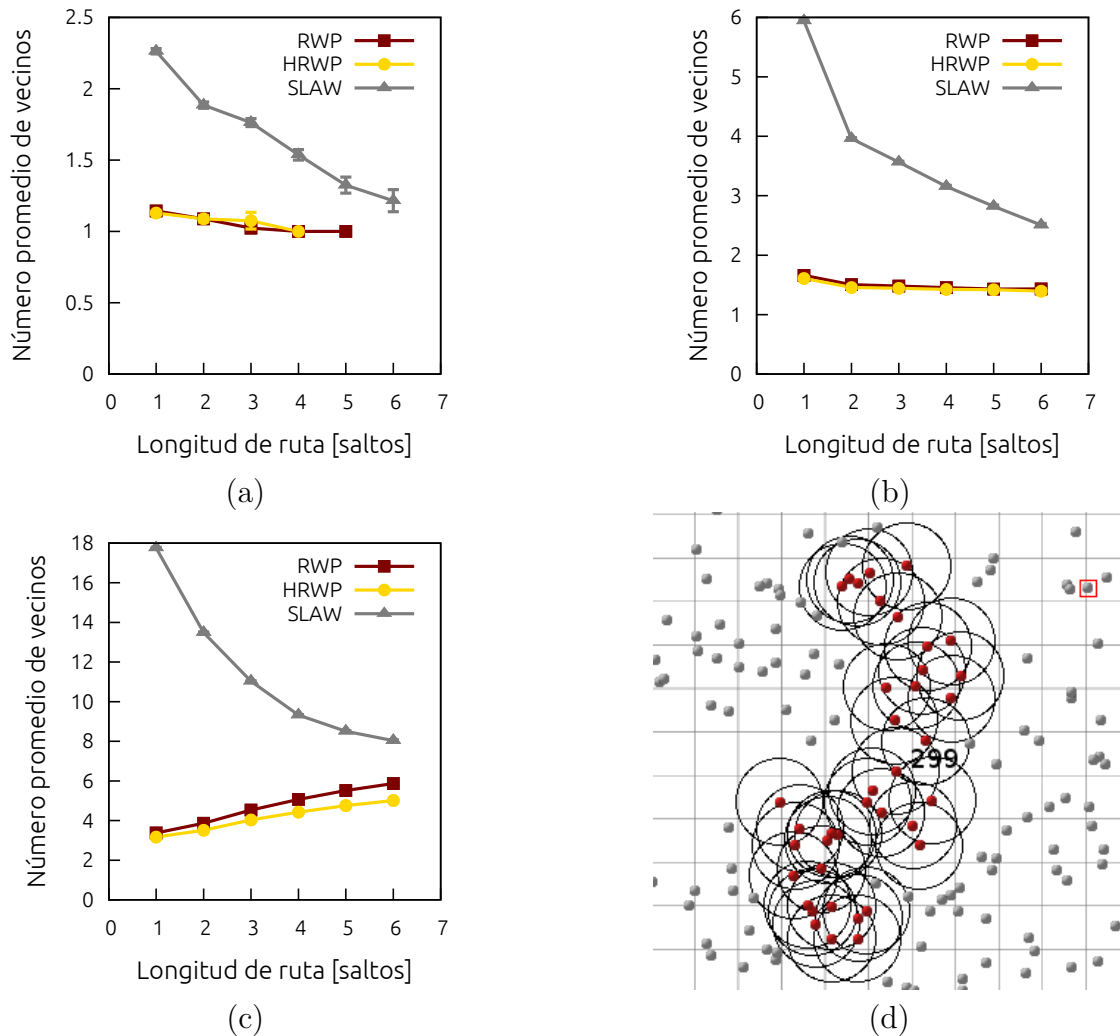


Figura 3.3: Número promedio de vecinos por salto en redes de (a) 25, (b) 100 y (c) 300 nodos. (d) Vecinos del nodo 299 hasta seis saltos en un escenario de red configurado con RWP y tamaño de red igual a 300 nodos.

ocurre porque los nodos forman pequeños grupos de radio igual a un salto que se conectan con otros por unos pocos nodos intermedios de tal forma que mientras mayor sea una ruta más nodos pueden ser alcanzados. El fenómeno se ilustra en la figura 3.3(d), en la que se observa que el nodo 299 puede alcanzar a distintos vecinos localizados a una distancia mayor que dos saltos a través de los dos únicos vecinos locales que tiene. Bajo el modelo SLAW, el número de vecinos disminuye conforme el número de saltos crece. No obstante, los nodos tienen más vecinos bajo el modelo SLAW que bajo las configuraciones del modelo RWP en

todos los casos y sin importar la distancia.

### 3.3.2. Desempeño de AODV

En este apartado, se explican los resultados de la evaluación hecha al protocolo AODV en términos de las medidas: razón de búsquedas exitosas, retardo de ida y vuelta, y tiempo de vida de la ruta.

En las figuras 3.4(a)-(c), se presenta la razón de búsquedas exitosas obtenidas de la observación de redes con distintos tamaños. Los valores promedio ahí mostrados incluyen intervalos con un nivel de confianza del 95 %. En las figuras, se muestra que el protocolo AODV puede establecer rutas entre vecinos a un salto con una probabilidad cercana a uno, indistintamente del modelo de movilidad empleado. No obstante, esta probabilidad decrece a razón del aumento de la distancia entre los nodos. En todos los casos, el protocolo AODV presenta el peor desempeño cuando los nodos se mueven de acuerdo con la configuración RWP. Un resultado interesante mostrado por estas figuras es que las configuraciones HRWP y SLAW presentan desempeños similares. Esto es debido a que la velocidad y el tiempo de pausa fueron tomados de las mismas distribuciones de probabilidad. Por lo tanto, puede inferirse que la razón de búsquedas exitosas únicamente depende de estos parámetros y no depende de los patrones de movilidad presentados por los nodos.

Adicionalmente, la figura 3.4(a) muestra que AODV no puede establecer rutas de una longitud mayor que tres saltos cuando los nodos siguen la configuración RWP y no mayores que dos saltos con la configuración HRWP. Esto puede parecer contradictorio porque hemos mencionado que bajo dichas configuraciones es posible alcanzar nodos a tales distancias. Sin embargo, para considerar que una búsqueda es exitosa se necesita que los nodos que componen la ruta por la que se envía la consulta conserven su misma conectividad al menos

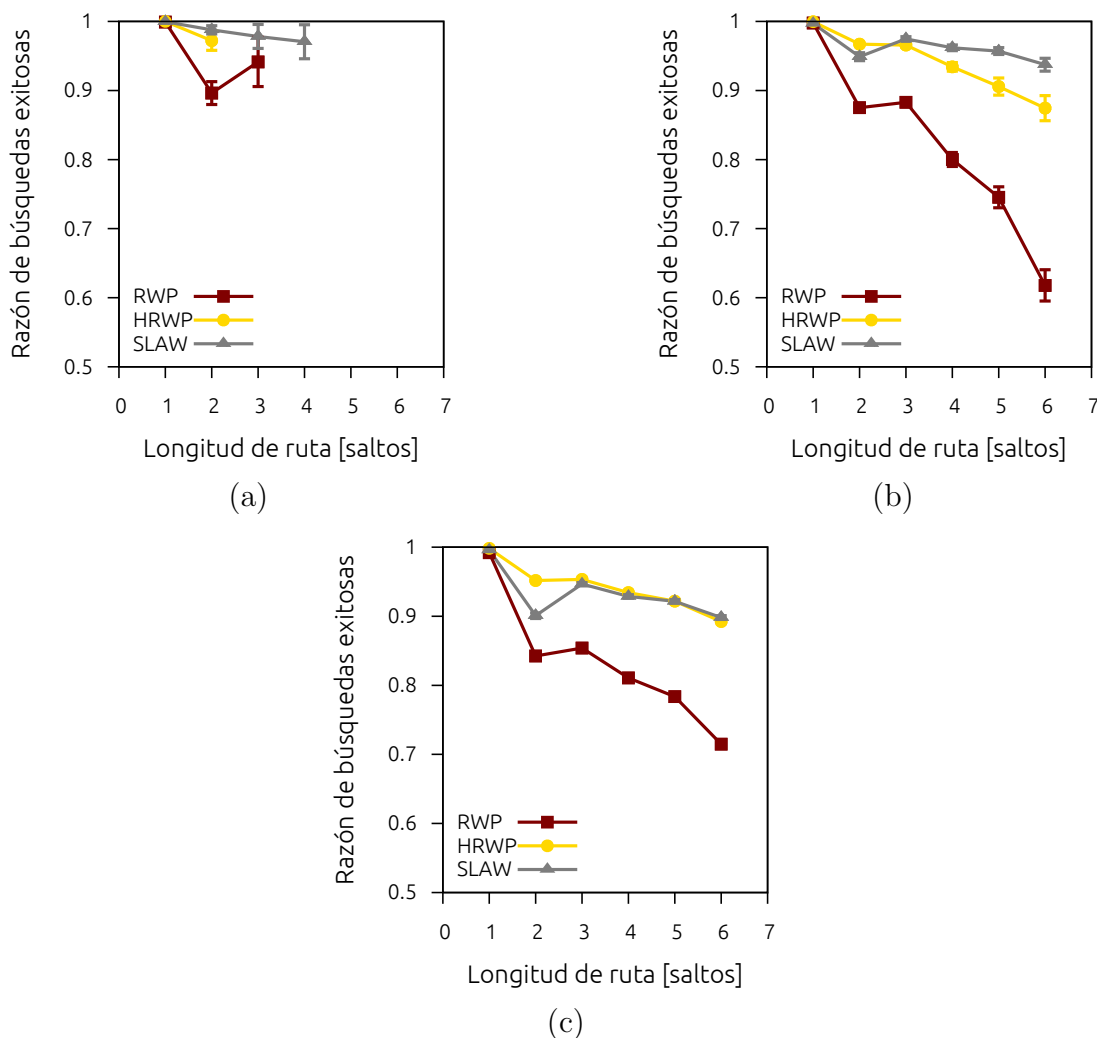


Figura 3.4: Razón de búsquedas exitosas medida en redes de (a) 25, (b) 100, (c) 300 nodos.

hasta que el nodo emisor reciba respuesta, lo cual no siempre ocurre.

Al evaluar el desempeño en términos del RTT, de manera general puede notarse que la medida no es afectada significativamente por los modelos de movilidad, como se observa en las figuras 3.5(a)-(c), donde los valores promedio incluyen intervalos de confianza con un nivel del 95%. La razón de esto es que la velocidad de los paquetes de datos es más rápida que la velocidad a la que se mueven los nodos. Por ello, se puede deducir que los modelos de movilidad empleados en estos experimentos no tiene mucha influencia en la medición del

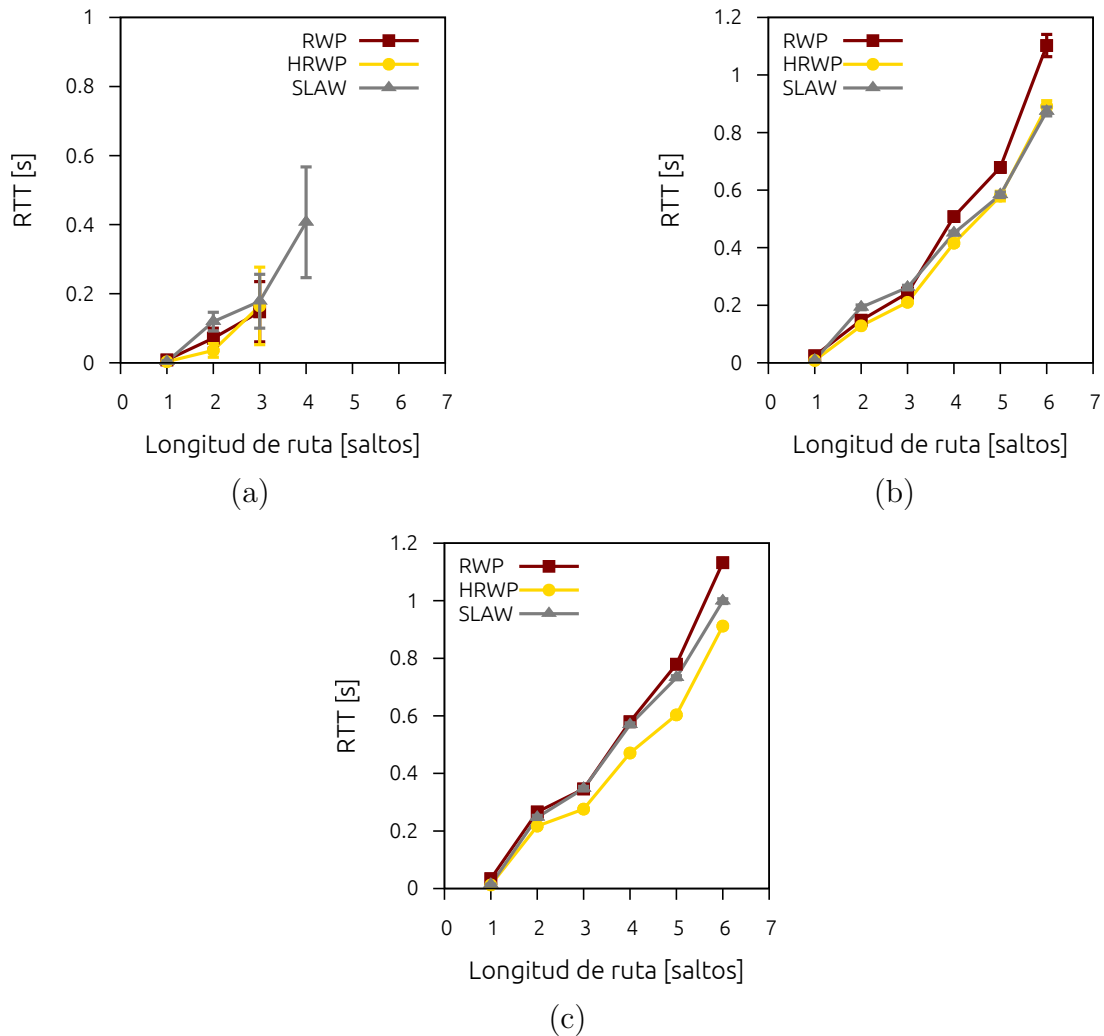


Figura 3.5: RTT medido en redes de (a) 25, (b) 100, (c) 300 nodos.

RTT. Además, como se esperaba, el retardo que exhibe el tiempo de llegada de la respuesta a una consulta se incrementa mientras que la longitud de la ruta aumenta. Por ejemplo, el RTT de rutas de longitud igual a un salto muestra un valor promedio próximo a 34.2 ms para una red de 300 nodos bajo la configuración RWP. Para el mismo caso, la medición promedio obtenida en rutas de seis saltos es próximo a 1.2 s. En adición, las tres figuras muestran que mientras más grande es el tamaño de la red, más grande es el RTT promedio medido. Claramente, esto se debe al incremento en la contención por el acceso al medio.

Un hecho interesante presentado en las figuras es la pequeña variación que ocurre con la medida en cuestión. En la figura 3.5(a), se observa que los nodos experimentan un RTT más largo bajo el modelo SLAW que bajo las configuraciones del modelo RWP. Esto se debe a que, como muestran los resultados antes explicados, bajo el modelo SLAW se obtiene la mayor razón de conectividad en una red de 25 nodos, lo que ocasiona que haya más contienda por el medio y, por lo tanto, las consultas exhiben un RTT un poco mayor. Sin embargo esta situación cambia en escenarios con tamaños de red mayores, como se observa en las figuras 3.5(b)-(c), donde el RTT más largo se obtiene bajo la configuración RWP, particularmente para rutas mayores que cuatro saltos. Esto se debe a que la red exhibe una mayor razón de conectividad bajo la dicha configuración en vecindarios localizados a tales distancias, como se ilustra en la figura 3.2(c).

Finalmente, se mide el tiempo de vida de las rutas establecidas por el protocolo AODV. Los resultados obtenidos de la ejecución de estos experimentos se presentan en las figuras 3.6(a)-(b) con intervalos con nivel de confianza del 95%. En ellas es posible notar que las rutas de longitud igual a un salto formadas bajo el modelo SLAW duran casi un orden de magnitud más que las establecidas bajo las configuraciones del modelo RWP. El alto desempeño que presenta AODV bajo el modelo SLAW se debe a la restricción de la movilidad dentro de las áreas confinadas. A su vez, en las figuras se nota que el tiempo de vida de ruta decrece mientras aumenta la distancia entre los nodos. En el caso de las configuraciones RWP y HRWP, el desempeño de AODV permanece casi constante independientemente de la longitud de la ruta. En contraste, el tiempo de vida de las rutas decrece casi exponencialmente bajo el modelo SLAW. Aun ante esta tendencia, el tiempo de vida de las rutas es mucho mayor bajo el modelo SLAW que bajo las configuraciones RWP y HRWP.

Particularmente, la figura 3.6(a) muestra que las rutas de cuatro saltos tienen una duración promedio aproximada de 400 s bajo SLAW, mientras que no es posible establecer rutas a



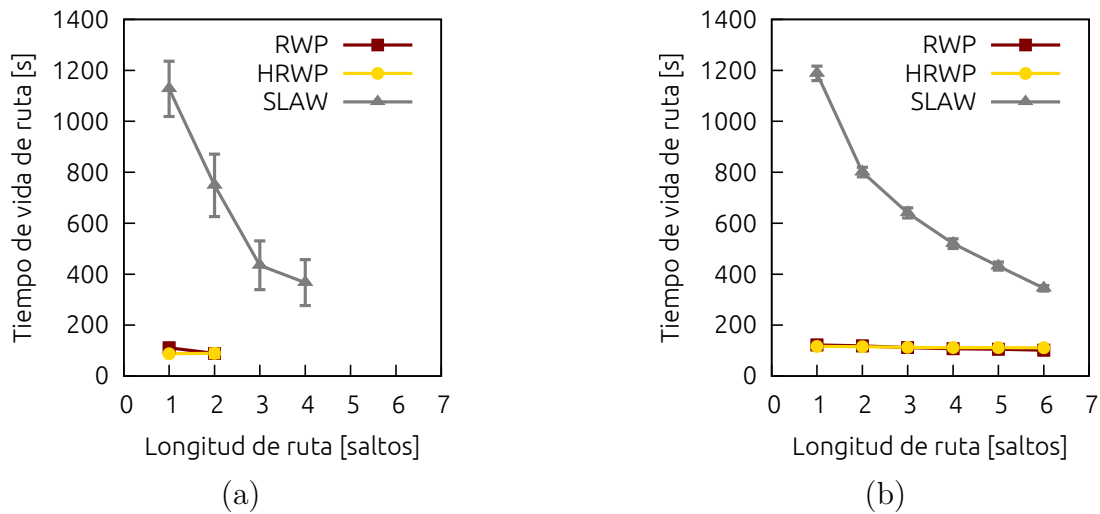


Figura 3.6: Tiempo de vida de las rutas creadas por el protocolo AODV medido en redes de (a) 25, (b) 300 nodos.

dicha distancia mediante las otras configuraciones. Además, en la figura se observa que la distancia máxima que pueden alcanzar las rutas bajo las configuraciones RWP y HRWP es de dos saltos. No obstante, los resultados de conectividad indican que es posible establecerse rutas entre nodos a tres saltos de distancia bajo tales configuraciones. Esto se debe a que los nodos no mantienen su conectividad durante el lapso necesario para medir su tiempo de vida debido a la granularidad del tiempo de observación. En el caso de redes compuestas por 300 nodos, cuyos resultados se muestran en la figura 3.6(b), puede notarse que el desempeño de AODV es aproximadamente tres veces mayor bajo SLAW que el obtenido con las otras configuraciones.

Con el objetivo de explicar por qué el modelo de movilidad influye en el desempeño mostrado por los protocolos de redes ad hoc móviles, vale la pena observar las figuras 3.1(a)-(b) donde se muestra el recorrido realizado por un nodo siguiendo el modelo SLAW y el modelo RWP, respectivamente. Contrastando ambas figuras es posible deducir que los enlaces inalámbricos cambian con menor frecuencia bajo el primero que bajo el segundo, esto debido a que los desplazamientos que experimenta un nodo al seguir el modelo RWP son más largos porque

la movilidad no está restringida, lo cual se agrava considerando radios de cobertura cortos (50 m en nuestro caso). En cambio, en la figura 3.1(b) se puede observar que muchos de los desplazamientos son cortos y otros pocos son largos, tal como se esperaba dado que los recorridos tienen una distribución de cola pesada bajo el modelo SLAW. Esta característica hace que la topología de la red física no cambie tan abruptamente como en el caso del modelo RWP.

### 3.4. Discusión

En este capítulo se analizaron las características de la topología de red inducida por los modelos de movilidad RWP y SLAW. Esto se hizo midiendo la razón de conectividad, la razón de aislamiento y el número promedio de vecinos a  $d$  saltos. A partir de dicho análisis, se encontró que la red exhibe una razón de conectividad alta al emplear como modelo de movilidad a SLAW, mientras que se observó lo contrario cuando los nodos se mueven de acuerdo con el modelo RWP. Esto indica que, en términos generales, las redes móviles conformadas por usuarios pedestres tienen más prestaciones que las que se han reportado en [58, 59].

En adición, se midió el desempeño del protocolo AODV bajo los modelos de movilidad SLAW y RWP. Los resultados indican que, contrariamente a lo que ha sido supuesto, la movilidad no es tan problemática al considerar las características estadísticas del movimiento humano. Estos resultados permiten avanzar en la dirección propuesta en [1] y [2], donde se menciona que las redes ad hoc móviles de propósito general carecen de aplicabilidad a menos que las restricciones que se asumen de ellas se relajen; en este caso, la movilidad puramente aleatoria.

Con base en los resultados aquí presentados, se intuye que las redes ad hoc móviles pueden prestar un servicio de búsqueda basado en redes lógicas si las características estadísticas del movimiento humano son tomadas en cuenta. Esto debido al nivel de conectividad y el tiempo

de vida de ruta que se obtuvo usando el modelo SLAW. Además, el tiempo de vida de ruta que se reporta en esta tesis doctoral indica que se puede diseñar un servicio de búsqueda P2P que verifique la validez de los enlaces lógicos después de varios minutos o que los restablezca hasta que fallen, sin afectar gravemente la razón de búsquedas exitosas. El desempeño de este protocolo podría verse beneficiado si tuviese un mecanismo que le permitiera establecer un enlace lógico entre dos terminales sin hacer que éste dependa de un conjunto particular de encaminadores, tal como pasa cuando se usa AODV en la capa de red. Esta estrategia de diseño se justifica por el hecho de que los nodos tienen una cantidad de vecinos significativa, lo que hace posible que exista más de un conjunto de ellos que pueda comunicar a un par de terminales.

Finalmente, cabe resaltar que no todas las características de la topología física pueden explotarse de la misma manera que es seguida en las redes P2P con infraestructura fija. Por ejemplo, el estado de los nodos podría organizarse como el de Kademlia para aprovechar el hecho de que el tiempo de pausa se modela con una distribución de cola pesada, lo que hace posible que existan terminales que permanezcan estáticas por un período considerable de tiempo. No obstante, no es posible asegurar el éxito de la estrategia ya que tales nodos no son alcanzables entre sí cuando están distribuidos geográficamente.



## Capítulo 4

# Análisis de estrategias estabilizantes para redes jerárquicas

Los protocolos de agrupamiento son empleados en las redes ad hoc móviles para hacer frente a su dinamicidad y caudal de datos limitado [31, 77]. Estos protocolos forman una red jerárquica producto de dividir la red inalámbrica en grupos adyacentes integrados por nodos que realizan distintas funciones. Normalmente, los grupos se componen de una única cabeza de grupo (*clusterhead*), de algunas pasarelas (*gateways*) y de varios miembros de grupos (*clustermembers*). Las cabezas de grupo son nodos que gestionan la organización de los grupos de manera centralizada. Los nodos con este rol almacenan en su estado al menos la identidad de todos los miembros que integran su grupo. Además, tienen la misión de proveer servicios a sus miembros, p. ej., pueden prestar los servicios de búsqueda [78] y de encaminamiento [29, 30]. Las cabezas de grupo establecen enlaces lógicos entre ellas usando nodos pasarelas cuyos enlaces inalámbricos interconectan dos o más grupos. Los miembros de grupo son nodos afiliados a una cabeza a la que le hacen llegar las solicitudes por servicios, ya sean propias o de otros nodos vecinos.

En la literatura, se ha demostrado que agrupar una red es ventajoso. Por ejemplo, en [79] se presenta el *sincronizador*  $\gamma$ : un protocolo que permite simular una red síncrona en una asíncrona. Para ello, este protocolo divide la red en grupos donde el líder se encarga de coordinar los eventos que pasan en su grupo y de informar la completitud de una ronda de ejecución a sus líderes vecinos. Bajo esta organización, este protocolo ofrece un buen equilibrio entre tiempo de ejecución y costo de comunicación en comparación con la versión totalmente distribuida (*sincronizador*  $\alpha$ ) que incurre en sobrecarga de mensajes y la versión centralizada (*sincronizador*  $\beta$ ) que requiere de mayor tiempo para completar su función.

Evidencia específica de las mejoras de desempeño que las redes jerárquicas pueden proveer en redes ad hoc móviles se muestra en [29] y en [30], donde se compara el rendimiento del protocolo de encaminamiento basado en grupos (*clustering-based routing protocol*, CBRP [80]) contra el de los protocolos de encaminamiento AODV [68], presentado en el apartado 3.1.2, y DSDV [81] (*destination-sequenced distance-vector*) en términos de confiabilidad y costo de mantenimiento. En cuanto al servicio de búsqueda, las solicitudes hechas sobre una red jerárquica no se transmiten a cada nodo de la red, sino que se dirigen directamente a la cabeza del grupo donde se genera la petición. Si la cabeza de grupo local no puede resolver la consulta, entonces la envía directamente a las cabezas de grupo vecinas a través de las pasarelas y así sucesivamente. Evidentemente, este esquema es más eficiente que el de la búsqueda no estructurada ya que requiere de una menor cantidad de nodos para realizar su función. De hecho, las consultas son resueltas contactando a un único líder en el mejor de los casos.

Las ventajas de dividir una MANET en grupos sólo se obtienen si la red lógica se encuentra correctamente conectada, es decir, cuando los miembros de grupo están al alcance de la cabeza de grupo que les corresponde y cuando las cabezas de grupos no establecen enlaces físicos entre ellas. Sin embargo, lo anterior puede no cumplirse debido a la movilidad de

los nodos, lo que provocará que el servicio provisto por la red lógica presente problemas de desempeño. En el caso de un servicio de búsqueda ocurre lo siguiente. Si los miembros no están correctamente afiliados, entonces el estado de las cabezas de grupo será incorrecto y el servicio de búsqueda presentará tanto falsos positivos como negativos. Los falsos positivos ocurren cuando las cabezas de grupo responden positivamente a una solicitud por un miembro de grupo que ya no está a su alcance. El caso complementario ocurre cuando una cabeza de grupo responde negativamente por un nodo que sí se encuentra en su grupo. A su vez, si las cabezas de grupo establecen enlaces físicos entre ellas, entonces sus comunicaciones se interferirán continuamente en escenarios donde los miembros de grupo generan solicitudes por recursos concurrentemente.

Al igual que las tablas *hash* distribuidas, los enlaces incorrectos de las redes jerárquicas se corrigen por un protocolo de autoorganización. Dicho protocolo hace que las cabezas de grupo actualicen su estado con regularidad. Además, el protocolo de autoorganización mezcla a los grupos cuyas cabezas hayan establecido un enlace incorrecto, disolviendo a un grupo y reafiliando a sus ex miembros para ello. Los procedimientos llevados a cabo por el protocolo de autoorganización, especialmente el segundo, requieren del intercambio de un gran número de mensajes de control, razón por la que su ejecución debe ser evitada siempre que sea posible ya que afecta severamente el desempeño del servicio provisto por la red P2P.

Las redes jerárquicas pueden reducir su costo de mantenimiento si evitan la desintegración y mezcla de los grupos en medida de lo posible. Para ello, deben ser *estables*, preservando su organización inclusive con la movilidad de los nodos. Esta propiedad se obtiene empleando estrategias estabilizantes que buscan mantener la organización original de la red jerárquica. Las estrategias estabilizantes pueden clasificarse en tres grupos:

1. *Criterios de elección de líder*. Su objetivo es dar el rol de cabeza de grupo a los nodos que de acuerdo con sus características, como velocidad y tiempo de pausa, tengan

mayor oportunidad de mantener la organización de la red. En [82–84] proponen emplear únicamente un criterio de elección mientras que en [85–88] se usa un conjunto de ellos para elegir a los organizadores.

2. *Políticas de validez relajadas.* Son medidas menos estrictas al determinar cuando dos cabezas de grupo se han interconectado incorrectamente, tal como se propone en [84, 89–91]. En [89], la política de validez consiste en permitir que cierto número de cabezas de grupo sean vecinos mientras que en [84] la política consiste en dejar que las cabezas de grupo puedan ser vecinas un cierto período de tiempo. Otro enfoque se presenta en [90, 91], donde el protocolo de agrupamiento crea grupos en los que los líderes están a una distancia de  $k$  saltos para reducir la probabilidad de que se establezca un enlace físico entre ellas.
3. *Políticas de reorganización local.* Éstas se aplican cuando se deja de cumplir una política de validez. Su objetivo es reparar localmente los enlaces incorrectos entre cabezas de grupo mediante la sustitución de una de las que afectaron la organización de la red por un miembro de su grupo. Este tipo de medidas evitan la desintegración de los grupos en última instancia.

Las estrategias estabilizantes son un factor de gran relevancia en el diseño de redes jerárquicas ya que afectan directamente el costo del mantenimiento de la red. En consecuencia, el efecto de dichas estrategias se ve directamente reflejado en el desempeño del servicio provisto por las cabezas de grupo. En el caso de un servicio de búsqueda, su confiabilidad queda directamente determinada por el éxito de las estrategias estabilizantes ya que las búsquedas fallan si la red jerárquica no está conectada correctamente.

En la literatura, se han presentado estudios donde miden indirectamente el rendimiento provisto por las estrategias estabilizantes mediante la evaluación del desempeño de protocolos



---

de agrupamiento [77, 92]. Además, en [93] se compara el desempeño dado por políticas de afiliación [94, 95] contra criterios de elección de líder [87] con el fin de determinar qué estrategia puede resultar más exitosa.

Las evaluaciones presentadas en el trabajo relacionado muestran la importancia de las estrategias estabilizantes en el desempeño de las redes de tipo jerárquico. Dado que en [93] sólo evalúan un pequeño subconjunto de ellas sin considerar su efecto agregado y que en [77] y [92] sólo las estudian indirectamente, en este capítulo se presenta una extensa evaluación de desempeño cuyo resultado determina el conjunto de estrategias estabilizantes que mantienen la organización de las redes lógicas de tipo jerárquico. A diferencia de las evaluaciones presentadas en otros trabajos, en la presentada en este capítulo se emplea el modelo de movilidad SLAW [32] para proveer un análisis de rendimiento más cercano a la realidad, ya que los resultados de desempeño de los protocolos de redes ad hoc móviles dependen en gran medida de la representación del movimiento de los nodos, tal como se mostró en el capítulo 3.

La evaluación de las estrategias estabilizantes se realiza de la siguiente manera. Primero se explican diversas estrategias estabilizantes en la sección 4.1. Después, en la sección 4.2 se presenta un marco de evaluación que permite medir el nivel de estabilidad que una red jerárquica obtiene al ser configurada con un conjunto de estrategias estabilizantes. Enseguida, se analizan los resultados de la evaluación de varias estrategias estabilizantes, explicando en primer lugar las características estadísticas de los grupos formados sobre una MANET donde el movimiento de los nodos representa estadísticamente el movimiento humano, después el nivel de estabilidad de las estrategias estabilizantes y finalmente el costo de mantener una red jerárquica. Todo esto se explica en la sección 4.3. Este capítulo cierra con la sección 4.4, donde se presenta una discusión sobre las ventajas y desventajas de proveer el servicio de búsqueda en redes ad hoc móviles empleando como sustrato una red lógica jerárquica.

## 4.1. Estrategias estabilizantes

Las estrategias estabilizantes tienen por objetivo preservar la organización de las redes jerárquicas ante la movilidad de los nodos, especialmente la de las cabezas de grupo. A continuación se explican ejemplos de estrategias que pertenecen a las tres clases descritas anteriormente.

### 4.1.1. Estrategias basadas en criterios de elección de líder

En una red jerárquica, las cabezas de grupo se determinan por medio de un criterio de elección de líder, p. ej., el del identificador único mínimo [96]. Además del anterior, pueden emplearse criterios más complejos basados en las características de los nodos que dependen de las condiciones de la red. Intuitivamente, las cabezas de grupo con esos atributos mejorarían la estabilidad de la red lógica, como se plantea en las siguientes propuestas.

Un criterio de elección de cabeza de grupo fácil de calcular es el del *grado máximo* [82, 83, 90]. Este criterio consiste en elegir como líder al nodo que localmente tenga la mayor cantidad de vecinos a un salto. Usando este criterio se forman grupos con un alto nivel de conectividad. En adición, al usar este criterio generalmente se eligen a los nodos que se encuentran en el centro de una red dado que es más probable que los nodos de la periferia tengan menos vecinos que los que se encuentran en el centro. Sin embargo, este criterio puede convertir a las cabezas de grupos en cuellos de botella si los miembros de grupo realizan solicitudes de manera concurrente ya que la contienda por el acceso al medio sería considerable. De acuerdo con [87], este problema puede evitarse si se considera la cantidad ideal de nodos que las cabezas de grupos pueden servir. Una extensión de este criterio se presenta en [97], en donde se propone discriminar a los nodos a través del número de vecinos que tengan dentro de un radio de  $k$  saltos.

En [87, 98, 99] proponen emplear la distancia entre nodos como factor discriminante con el fin de mejorar las comunicaciones entre las cabezas de grupo y sus miembros. Además, este criterio puede ser usado para detectar grupos móviles ya que intuitivamente los nodos que se mueven en grupo preservan cierta distancia entre ellos. Un ejemplo de criterio de elección basado en la distancia es la *mínima distancia promedio*, con el que se elegirán como cabezas de grupo a los nodos cuya distancia media a sus vecinos sea la mínima.

Otro atributo para elegir cabezas de grupo es la velocidad, la cual es empleada siguiendo distintos enfoques. Uno de ellos se basa en la intuición de que la red de cabezas de grupo sería más estable si sus integrantes exhiben una rapidez baja. Para este fin, se eligen a los nodos con la *rapidez promedio mínima* [86–88] como líderes. Este criterio tiene la desventaja de que sólo puede ser calculado si los nodos mantienen un historial del escalar en cuestión. Para evitar esto, se puede emplear como alternativa el criterio de la *rapidez actual mínima* que no requiere un registro para ser calculado. Otro de los enfoques es considerar la *velocidad relativa mínima* de los nodos. Este criterio es especialmente útil cuando se considera que las terminales se mueven en grupos porque la velocidad de los integrantes de un mismo cúmulo será muy similar. Su desventaja es que no es tan sencilla de obtener porque requiere el cálculo de la dirección de desplazamiento de los nodos.

En [85], se proponen dos criterios de elección basados en las características estadísticas del movimiento humano reportadas en [34]. El primero es el *superrecorrido mínimo* que elige a los nodos que hayan exhibido desplazamientos menores a una distancia dada. El segundo es la *superpausa máxima* que busca que los nodos que muestren pausas mayores a un tiempo dado sean elegidos como cabezas de grupo. Estos dos criterios se fundamentan en que los nodos con estas características de movimiento tenderán a permanecer por más tiempo en la misma área confinada. Al igual que con el criterio de la rapidez promedio, éstos tienen la desventaja de requerir que los nodos registren sus tiempos de pausa y longitudes de recorrido

para poder ser calculados.

En adición, las cabezas de grupo pueden ser elegidas mediante su tiempo de pausa actual. Siendo así, los nodos que localmente presenten el *menor tiempo de pausa* serán elegidos como líderes. La estrategia está basada en la intuición de que los nodos que acaban de detenerse tienen más probabilidad de permanecer inmóviles que los nodos que llevan un período tiempo corto sin moverse.

#### 4.1.2. Estrategias basadas en políticas de validez relajadas

La política de validez básica es la *política estricta* que establece que dos nodos con el rol líder no pueden ser vecinos. Esta política es difícil de acatar en escenarios móviles, por lo que en la literatura se han presentado diversas propuestas para relajar su cumplimiento mediante reglas que establecen la manera de interconectar cabezas de grupo.

La política que se presenta en [89] permite que un número predeterminado de cabezas de grupo puedan ser vecinas. Esta política hace que las cabezas de grupo se interfieran constantemente en escenarios donde los miembros generan un número alto de solicitudes de manera concurrente. Por lo tanto, esta política opera bien cuando el tipo de aplicación hace que los usuarios no soliciten servicios de manera concurrente.

La política propuesta en [84] busca tomar ventaja de las características de la movilidad en grupos, específicamente del hecho de que grupos de nodos pueden compartir una misma área confinada sólo por un período de tiempo, por lo que no es conveniente desintegrar su organización original para formar una red jerárquica nueva. Por ello, la política permite que las cabezas de grupos puedan ser vecinas hasta que se venza un temporizador previamente establecido. Si dos cabezas de grupo siguen preservando enlaces inválidos después del tiempo que se les permite, entonces se invoca al protocolo de autoorganización.

En [90], se propone que las cabezas de grupo mantengan una distancia de tres saltos entre sí para reducir el número de grupos que integran la red lógica y, por consiguiente, disminuir la probabilidad de no acatar la política estricta. Para poder establecer dicha red lógica se define el rol de *invitado* que se asigna a nodos que no se encuentran en el área de cobertura de una cabeza de grupo pero que pueden conectarse a alguna usando un miembro de grupo como nodo intermediario. La característica especial que tienen los invitados es que son los únicos que pueden formar grupos nuevos, esto cuando su vecindario únicamente se compone de otros invitados, cumpliéndose así la regla de mantener una distancia de tres saltos entre las cabezas de grupo.

Siguiendo una estrategia similar a la anterior, en [91] se propone que la red jerárquica se integre de grupos de radio  $k$ , así, mientras mayor sea  $k$ , menor será la cantidad de grupos. De acuerdo con los autores, la desventaja de esta política es que las operaciones de mantenimiento interno de los grupos pueden complicarse, p. ej., las notificaciones de líderes hacia los nodos localizados en la periferia del grupo pueden experimentar retardos largos. Esta situación puede empeorar si las cabezas de grupo no se encuentran en el centro de su grupo. Para hacer frente a este problema, se propone un mecanismo de señalización que monitoriza el grado de interconexión de las cabezas de grupo con sus miembros con el fin de reemplazar localmente a aquellas que presenten problemas de desempeño.

### 4.1.3. Políticas de reorganización local

En [91] y [100] se propone reemplazar a la cabeza de grupo por uno de sus nodos afiliados en lugar de desintegrarlo. Teniendo en cuenta que el servicio ofrecido por la cabeza de grupo sustituida no necesariamente se puede recuperar inmediatamente después del reemplazo, en [100] se sugiere que se mantenga un reemplazo que esté listo para prestar el servicio en el momento en que se requiera. Una desventaja de aplicar esta política es que no se considera

que el nodo de respaldo puede no cumplir la política de validez que le corresponda, lo que provocaría que la medida no corregiría la red. Además, los nodos de reemplazo pueden no estar en el centro del área de cobertura de su grupo, razón por la que las comunicaciones intragrupalas pueden verse afectadas [91].

## 4.2. Marco de evaluación

Todas las estrategias estabilizantes descritas anteriormente se diseñaron para mejorar el rendimiento exhibido por los protocolos de agrupamiento. Sin embargo, todavía no ha sido aclarado con cuál de estas estrategias se obtiene el mejor desempeño. Además, no se conoce cómo estas estrategias se desempeñan considerando modelos que representan estadísticamente la movilidad humana. Estas cuestiones son resueltas mediante una evaluación de desempeño en la que se mide el nivel de estabilidad dado por las estrategias estabilizantes, de manera individual y conjunta. En términos generales, la evaluación se hace en una red simulada donde los nodos son agrupados a través de un algoritmo capaz de configurarlos con un conjunto de estrategias estabilizantes. En adición, los nodos de red deambulan sobre un área siguiendo el modelo SLAW descrito en el apartado 3.1.1. Otros detalles del marco de evaluación también se explican a continuación.

### 4.2.1. Estrategias de estabilización evaluadas

Los criterios de elección de cabeza de grupo evaluados en esta tesis doctoral son: el grado máximo [82, 83, 90], el número máximo de vecinos a  $k$  saltos [97], la distancia mínima promedio, la rapidez mínima, el tiempo de pausa mínimo, el superrecorrido mínimo [85] y la superpausa máxima [85]. Con respecto a las últimas dos medidas, en este estudio se considera

que los nodos exhiben un superrecorrido cuando atraviesan una distancia mayor a 400 m en línea recta y que exhiben una superpausa cuando permanecen detenidos por más de 1200 s. Estos dos criterios se calculan mediante las fórmulas presentadas en [85].

Las políticas de validez evaluadas son:

- *Política de validez estricta.* Las cabezas de grupo no pueden permanecer en el vecindario a  $k$  saltos de otras. Siguiendo esta política, la red jerárquica es correcta cuando las cabezas de grupo están separadas entre sí por  $k + 1$  saltos, lo cual es una generalización de la política estricta presentada en el apartado 4.1.2.
- *Política de validez flexible.* Dado un parámetro de flexibilidad  $d$  medido en saltos, bajo esta política se considera que la red jerárquica es correcta si las cabezas de grupo preservan una distancia entre ellas de  $(k - d + 1)$  saltos. Debido a su definición, esta política conlleva a la política estricta con  $d = 0$ . Su funcionamiento es una generalización de las políticas presentadas en [90, 91].
- *Política de delegación de rol.* Cuando dos cabezas de grupo establecen un enlace inválido, se intenta reemplazar de manera reactiva a la que notó primeramente el incumplimiento de la política de validez por uno de sus vecinos que sí pueda cumplirla.

Las condiciones en las que no se cumplen las políticas de validez descritas arriba se ilustran en la figura 4.1. En ambas figuras, se muestran dos grupos con radio igual a dos saltos, uno etiquetado con la letra  $a$  y otro con la letra  $x$ , donde cada cabeza de grupo se representa con un círculo doble. En la figura 4.1(a), se muestra una red jerárquica incorrecta bajo la política estricta dado que las cabezas de grupo se encuentran separadas a dos saltos. No obstante, si la política flexible se aplica con  $d = 1$  a la misma red, entonces ésta sigue siendo correcta porque las cabezas de grupo se encuentran a una distancia mayor o igual que un

salto. Alternativamente, la red lógica de la figura 4.1(a) puede ser reparada si se aplica la política de delegación de rol. Para ello asumamos que la cabeza de grupo  $x$  se percata del establecimiento del enlace inválido, entonces tiene dos vecinos, etiquetados con  $x_1$  y  $x_2$ , a los que les puede delegar su función. Si la cabeza de grupo  $x$  delega el rol a  $x_1$ , entonces la red lógica seguirá siendo incorrecta, pero si le cede el rol al nodo  $x_2$ , entonces el enlace inválido será eliminado. Por lo tanto, el rol de cabeza de grupo se cede al nodo  $x_2$ . El resultado de esta reparación local se ilustra en la figura 4.1(b).

Las estrategias estabilizantes consideradas en este estudio se ordenan en *configuraciones* representadas por el cuarteto  $\mathcal{C} = \langle c, k, i, d \rangle$ , donde  $c$  es un criterio de elección de líder,  $k$  es el radio máximo de los grupos,  $i$  es un parámetro binario que indica si la política de delegación de rol está siendo aplicada o no ( $\neg i$ ), y  $d$  es el parámetro de flexibilidad. Con el fin de facilitar la nomenclatura, el valor del radio de grupo y del parámetro de flexibilidad se indican en el subíndice de los parámetros  $k$  y  $d$ . Siendo así, el elemento de la configuración que denota un radio de grupo igual a dos saltos es  $k_2$ . Las configuraciones donde  $k \leq d$  son

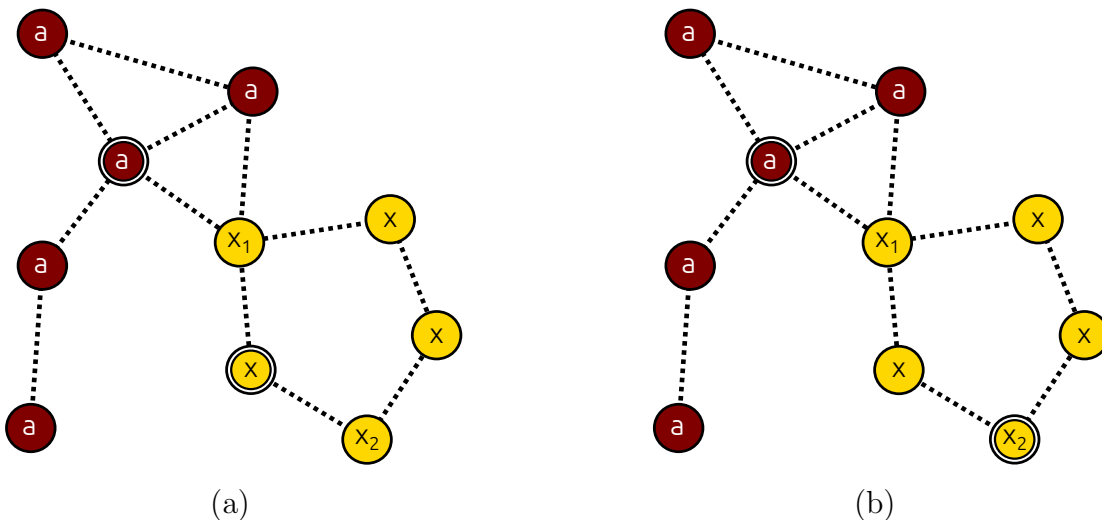


Figura 4.1: (a) Red inválida bajo la política estricta, pero válida bajo la política flexible. (b) Red lógica mostrada en la figura (a) corregida empleando la política de delegación de rol con  $k = 2$  y  $d = 1$ .



inválidas porque no cumplen con la definición de las estrategias aquí tratadas.

La manera en la que se observa el efecto particular de un elemento de la configuración es la siguiente. Los efectos de un criterio de elección de cabeza de grupo  $c$  en la red jerárquica se miden variando el valor de  $c$  y manteniendo fijo el valor de los elementos restantes de la configuración  $(k, i, d)$ . Los efectos de las políticas de validez se analizan a la inversa, es decir, manteniendo fijo el valor de  $c$  y variando las combinaciones posibles de los elementos que representan las políticas. De esta manera, los efectos de la política estricta pueden observarse al usar configuraciones con elementos  $\neg i$  y  $d_0$ . De manera similar, los efectos de la política de delegación de rol pueden medirse en configuraciones con parámetros  $i$  y  $d_0$ . El caso de la política flexible se presenta únicamente con las configuraciones con parámetro  $d_1$ . Finalmente, las configuraciones del tipo  $\langle c, k_2, i, d_1 \rangle$  corresponden a los casos donde se aplica la flexibilidad y la delegación de rol de manera conjunta. En este análisis sólo se estudian configuraciones con  $k_1$  y  $k_2$ , por lo que los efectos del radio del grupo pueden observarse fijando los parámetros  $c$ ,  $i$ , y  $d_0$ . Debido a su formulación, los efectos del criterio de elección basado en el número máximo de vecinos a  $k$  saltos y de la política flexible sólo pueden observarse en configuraciones con parámetro  $k_2$ .

### 4.2.2. Algoritmo de agrupamiento

En esta evaluación, distintas estrategias estabilizantes se comparan de manera justa. Para ello, en lugar de evaluarlas empleando los protocolos de agrupamiento donde se aplican originalmente, se emplea uno capaz de ser ajustado de acuerdo con una configuración  $\mathcal{C}$  dada. De manera general, el algoritmo 1 construye y mantiene una red lógica jerárquica mediante el acatamiento del conjunto de reglas que corresponden a la configuración  $\mathcal{C}$ .

El algoritmo 1 toma por entrada el conjunto de nodos  $V$  que conforma la red y con esa

información comienza por calcular el vecindario a  $k$  saltos de cada uno de los nodos. Después de eso, el algoritmo 1 ejecuta el procedimiento  $OrganizeIsolatedNodes(V)$  que asigna la etiqueta *aislado* a los nodos sin vecinos y corrige la de los nodos que ya no lo están. Estos nodos son etiquetados como *desagrupados*.

Enseguida, se verifica que los nodos agrupados tengan el rol que les corresponde mediante el procedimiento  $OrganizeClusteredNodes(V, \mathcal{C})$ . En principio, el procedimiento se encarga de conectar a los miembros con la cabeza de grupo más cercana. En caso de que existan varias opciones, entonces los miembros eligen al líder con mayor *aptitud*, donde la aptitud es un valor relacionado con el criterio de elección, p. ej., cuando se usa el criterio del grado máximo, entonces la aptitud de las cabezas de grupo será igual al número de sus vecinos. El procedimiento también asigna la etiqueta de desagrupado a los nodos agrupados que no tienen un líder con quien afiliarse.

Lo siguiente en realizarse es verificar el estatus de las cabezas de grupo mediante el procedimiento  $OrganizeClusterheads(V, \mathcal{C})$  que aplica las medidas que correspondan a la configuración  $\mathcal{C}$  sin desintegrar grupos inválidos. Los nodos de los grupos que son desintegrados son etiquetados como desagrupados. Al igual que en [101], el procedimiento permite que las cabezas de grupo preserven su rol siempre que su grupo cumpla las políticas contenidas en  $\mathcal{C}$ .

---

**Algoritmo 1**  $Clustering(V)$ 


---

```

1: when  $clock = alarm$ 
2: begin
3:    $ComputeNeighborhood(V, k)$ 
4:    $OrganizeIsolatedNodes(V)$ 
5:    $OrganizeClusteredNodes(V, \mathcal{C})$ 
6:    $OrganizeClusterheads(V, \mathcal{C})$ 
7:   for all  $node\ v \in V \mid Role(v) = unclustered$  do
8:      $w \leftarrow ComputeClusterhead(v, \mathcal{C})$ 
9:      $BuildCluster(w, \mathcal{C})$ 
10:  end for
11:   $alarm \leftarrow alarm + t$ 
12: end

```

---

Finalmente, el algoritmo construye grupos de nodos desagrupados valiéndose de los procedimientos  $ComputeClusterhead(v, \mathcal{C})$  y  $BuildCluster(v, \mathcal{C})$ , que reciben como entrada un nodo que pertenece a  $V$  y una configuración. El procedimiento  $ComputeClusterhead(v, \mathcal{C})$  regresa la cabeza de grupo más cercana a  $v$ . En caso de que existan varias opciones, el procedimiento regresa la cabeza con la mayor aptitud. Si el empate persiste, entonces éste se rompe con el identificador único. Si no existen cabezas de grupo cercanas a  $v$  y éste es el único nodo desagrupado en su vecindario a  $k$  saltos, entonces  $v$  se convierte en cabeza de grupo. De otra manera, el procedimiento regresa un nodo desagrupado  $w$  que es alcanzable por  $v$ , que tiene la aptitud más alta de su vecindario a  $k$  saltos y que no invalida ningún grupo vecino. El procedimiento en cuestión eventualmente regresará un nodo que puede agrupar a  $v$ ; de hecho puede regresar a  $v$ . Una vez que se determina el nodo desagrupado que se convertirá en cabeza de grupo, el procedimiento  $BuildCluster(v, \mathcal{C})$  forma un grupo nuevo a partir de  $v$ . Esto se hace asignando el rol de cabeza de grupo a  $v$  y el rol de agrupado a los nodos desagrupados que pertenezcan al vecindario a  $k$  saltos de  $v$ . En adición, el procedimiento afilia a los nodos del vecindario a  $k$  saltos de  $v$  que estén más próximos a  $v$  que a su cabeza de grupo actual. El Algoritmo 1 se ejecuta periódicamente cada  $t$  segundos con el fin de mantener actualizada la red jerárquica.

### 4.2.3. Medidas de evaluación

Las siguientes medidas se emplean para cuantificar las características estadísticas de los grupos que integran la red jerárquica configurada según una configuración  $\mathcal{C}$  dada.

- *Tamaño de grupo.* Esta medida cuantifica el número de elementos que componen un grupo. Determina si una cabeza de grupo puede ser potencialmente un cuello de botella.
- *Número de grupos.* Simplemente es el número de grupos que integran la red jerárquica.

Las medidas siguientes se emplean para cuantificar el nivel de estabilidad provisto por las estrategias antes presentadas.

- *Tiempo de vida de grupo.* Es el tiempo  $T_{\text{cluster}}$  que un grupo dura organizado. Comienza desde el instante  $t_{\text{init}}$  que la cabeza de grupo es elegida hasta el momento  $t_{\text{break}}$  en el que se desintegra un grupo por el incumplimiento de una política de invalidación. Mientras mayor sea el tiempo de vida exhibido por los grupos, mayor será la estabilidad provista por la estrategia. Se calcula mediante la fórmula:

$$T_{\text{cluster}} = t_{\text{break}} - t_{\text{init}} \quad (4.1)$$

- *Razón de desintegración.* Denotada por  $D_r$ , es el número de desintegraciones  $d$  de grupo ocasionadas por el incumplimiento de una política de validez  $d_{\text{invalidation}}$  o el aislamiento de la cabeza de grupo  $d_{\text{isolation}}$  entre el número total de desintegraciones  $d_{\text{total}}$ . Una razón de invalidación alta indica que el mantenimiento de una estructura lógica jerárquica es costoso. Su cálculo se realiza con la fórmula

$$D_r = (d_{\text{invalidation}} + d_{\text{isolation}})/d_{\text{total}} \quad (4.2)$$

La última medida empleada en este análisis es la tasa de reafiliaciones  $R_r$  que cuantifica el costo asociado a aplicar una configuración determinada. Se calcula contando el número de reafiliaciones por unidad de tiempo. Las reafiliaciones se clasifican según su origen para distinguir las debidas a la movilidad de las que son causadas por la desintegración de un grupo.

#### 4.2.4. Configuración de las simulaciones

La evaluación descrita en este capítulo se realiza por medio de simulaciones de eventos discretos. El escenario simulado es un área de  $1000 \times 1000 \text{ m}^2$  que representa el tamaño típico de un campus universitario sobre el que deambulan nodos inalámbricos siguiendo el modelo de movilidad SLAW [32]. La configuración de SLAW empleada en estos experimentos es la misma que la que se presenta en el apartado 3.2.2. En cada experimento, se configura el número de terminales inalámbricas tomando valores del conjunto  $\{25, 50, 100, 150, 200, 300\}$ . Además, el área de cobertura de cada terminal se fija con un valor de 50 m.

El escenario de evaluación se implementa en el simulador INET 2.5 [42] basado en OMNeT++ versión 4.6 [43]. Durante la primera etapa, se obtienen muestras para calcular los criterios de superrecorrido y superpausa. En la segunda etapa, se recolectan datos para calcular las medidas de desempeño. En el caso del tamaño del grupo, el número de grupos y la tasa de reafiliaciones, los datos se obtienen cada segundo de simulación para poder obtener promedios representativos de un conjunto grande de muestras. En el caso de las medidas relacionadas con la estabilidad, los datos se colectan cada vez que ocurre una desintegración de grupo. La duración de la primera y segunda etapa es de 10 y 72 horas de simulación.

Además, el algoritmo 1 se ejecuta cada vez que el tiempo de simulación es igual al valor de *alarm* que se actualiza en el paso once al aumentarse su valor actual en  $t$  unidades de tiempo, esto con el fin de organizar continuamente la red lógica. La variable  $t$  se configura con un valor de 1 s para todos los experimentos aquí presentados.

En la simulación, no se modela la comunicación entre los nodos debido a que esta evaluación de rendimiento tiene por objetivo medir la estabilidad dada por distintas estrategias estabilizantes. Por esta razón, no se toma en cuenta el rol de pasarela.

## 4.3. Resultados

En esta sección, se analizan a detalle los efectos de las estrategias estabilizantes en las redes jerárquicas. Primero, se describen las características estadísticas de las redes resultantes de establecer grupos sobre un mapa de puntos de recorrido distribuidos de manera autosimilar. Después, se analiza el nivel de estabilidad que exhiben las estrategias autosimilares y, finalmente, se explican los resultados relacionados con el costo de soportar una red jerárquica, construida y mantenida según una configuración  $\mathcal{C}$ , sobre una red ad hoc móvil.

### 4.3.1. Características estadísticas de la red jerárquica

El primer hecho a resaltar de los resultados aquí presentados es que los criterios de elección de líder afectan de igual manera a las características estadísticas del tamaño de los grupos y su número. Esto significa que la posición espacial de las cabezas de grupo, la cual varía con respecto al criterio de elección, no produce cambios importantes en las medidas en cuestión. Esto es debido a que los grupos se establecen dentro de áreas confinadas donde el espacio limitado sólo permite que una cierta cantidad de ellos pueda formarse sin importar la posición geográfica de las cabezas de grupo. De hecho, las características del escenario simulado hacen que un grupo de radio uno sea suficiente para abarcar toda un área confinada que se expande a lo más 40 m a la redonda, esto porque el área de cobertura de las terminales móviles es de 50 m.

En contraste con el hecho arriba mencionado, los parámetros  $k$ ,  $i$  y  $d$  de las configuraciones examinadas sí modifican las características estadísticas en cuestión, como se ilustra en la figura 4.2. De manera esperada, la figura 4.2(a) muestra que el tamaño de los grupos crece conforme aumenta el tamaño de la red. Además, la figura muestra que el tamaño de los grupos construidos bajo las configuraciones en las que se aplica la política de flexibilidad

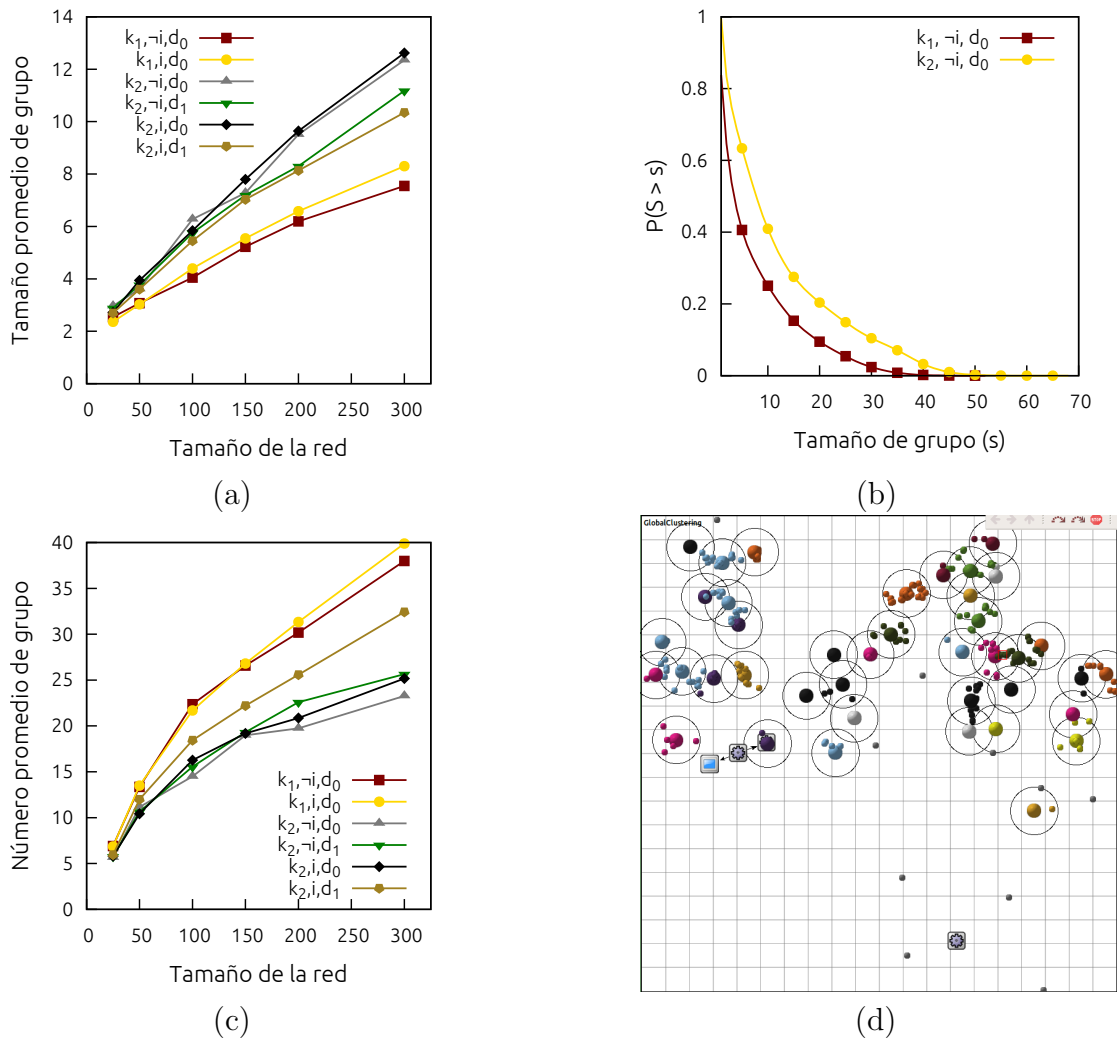


Figura 4.2: Resultados que describen las características estadísticas de los grupos bajo el modelo de movilidad SLAW. (a) Tamaño promedio. (b) CCDF del tamaño de los grupos. (c) Números promedio de grupos. (d) Red jerárquica de 300 nodos formada bajo la configuración  $(k_2, \neg i, d_0)$ .

(configuraciones con parámetro  $d_1$ ) es menor que el de las otras configuraciones con parámetro  $k = 2$ . Esto se debe a que las reglas de construcción de grupos que corresponden a las configuraciones con parámetro  $d = 1$  permiten la creación de grupos de radio uno ya que la política flexible deja que las cabezas de grupo preserven su rol aunque otras cabezas estén a dos saltos, lo que indirectamente forma grupos de radio uno.

La figura 4.2(b) muestra la función de distribución complementaria que modela el tamaño de

los grupos de redes jerárquicas de 300 nodos formadas bajo las configuraciones con parámetros  $(k_1, \neg i, d_0)$ , y  $(k_2, \neg i, d_0)$ . Al observar estas funciones es posible notar que existe la probabilidad de formación de grupos de tamaño considerable, esto sin importar el valor del parámetro  $k$ . Tal probabilidad es baja pero no insignificante, p. ej., la probabilidad de que se formen grupos de tamaño mayor que 25 nodos para grupos de radio uno es de 0.05. Para el caso de los grupos de radio dos la misma probabilidad es aproximadamente de 0.15. Estas mediciones son consecuencia de la propiedad de la movilidad humana que establece que tendemos a aglomerarnos en áreas populares (ver apartado 3.1.1). Este resultado no se habría podido apreciar si se hubieran empleado otros modelos de movilidad tales como RWP o RW (*random walk*) dado que éstos no representan la propiedad antes enunciada.

El efecto que causa el radio de agrupamiento  $k$  en el número de grupos se muestra en la figura 4.2(c), donde es posible notar que las curvas que corresponden a las configuraciones con parámetro  $k_2$  están por debajo de las de  $k_1$ . Básicamente, esto se debe a que los grupos de radio dos abarcan más nodos que los de radio uno. Por ello, las redes jerárquicas formadas bajo la política estricta aplicada a grupos de radio dos son las que exhiben la menor cantidad de grupos. Un hecho interesante ilustrado en la figura 4.2(c) es que el número de grupos que se producen bajo la configuración  $\langle \text{maxgrado}, k_2, i, d_1 \rangle$ , es significativamente mayor que el producido por las demás configuraciones con parámetro  $k_2$ . Esto ocurre debido a que la política de flexibilidad junto con la de herencia buscan preservar los grupos en lugar de desintegrarlos, lo cual se refleja en la cantidad que hay de ellos en la red.

En la figura 4.2(d), se muestran los grupos establecidos sobre el mapa de puntos de recorrido ilustrado en la figura 3.1(a). En esta figura, las cabezas de grupo se representan con esferas de tamaño mayor que las de sus miembros de grupo, los cuales tienen el mismo color que su líder. Las esferas en color gris representan nodos aislados. Estos grupos se construyen bajo la configuración  $\langle \text{maxgrado}, k_2, i, d_1 \rangle$ . Por medio de estas dos figuras se puede notar la



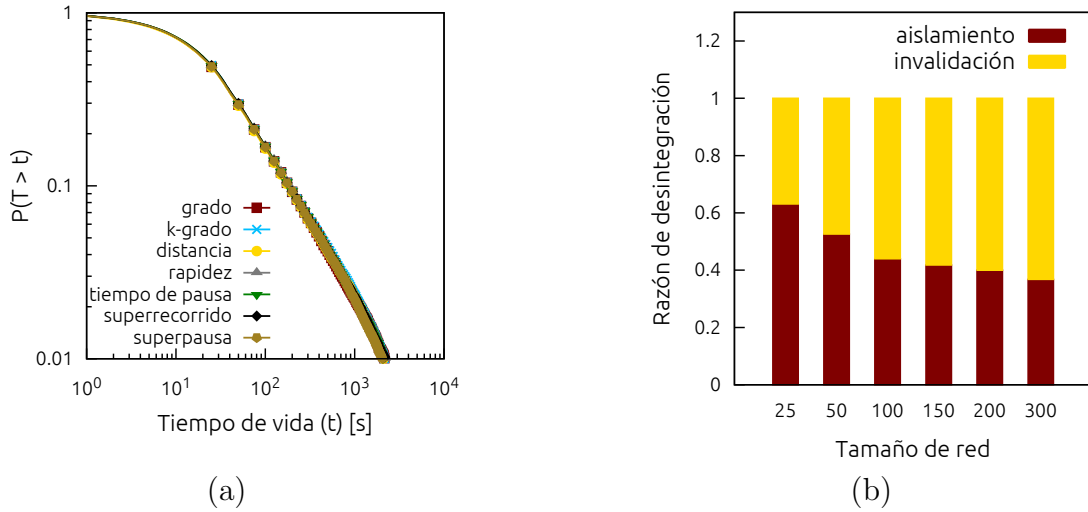


Figura 4.3: Nivel de estabilidad provisto por distintos criterios de elección de cabezas de grupo. (a) CCDF del tiempo de vida de grupo ( $T_{\text{cluster}}$ ). (b) Razón de desintegración  $D_r$  debida a invalidaciones y aislamiento de cabezas de grupo.

dependencia entre el tamaño de los grupos y el número de puntos de recorrido que integran el área confinada donde se forman. Siendo así, los grupos grandes tienen alta probabilidad de formarse sobre áreas populares. También, en la figura es posible notar que existen nodos que permanecen aislados porque se establecieron en áreas con una baja densidad de puntos de recorrido.

### 4.3.2. Estabilidad de la red jerárquica

El nivel de estabilidad provisto por los distintos criterios de elección de cabezas de grupo en una red de 300 nodos bajo los parámetros de configuración  $k_2, \neg i, d_0$  se muestra en la figura 4.3.

Un resultado sorprendente obtenido de estos experimentos es que los criterios de elección de líder exhiben aproximadamente el mismo desempeño. Inclusive el superrecorrido y la superpausa que están diseñados para aprovechar algunas propiedades del movimiento humano, no

extienden el nivel de estabilidad más allá que los demás criterios. Este resultado se ilustra en la figura 4.3(a), donde se muestra que las curvas que corresponden a cada criterio de elección no presentan variaciones importantes entre ellas. Este resultado sugiere que se puede hacer uso de criterios de elección de líder de fácil cálculo sin sacrificar desempeño. Los resultados de escenarios con tamaños de red menores presentan la misma tendencia pero con un nivel de desempeño más alto. En adición, la figura 4.3(a) muestra que la probabilidad de que los grupos exhiban tiempos de vida largos es baja, p. ej., la probabilidad de que un grupo se mantenga por más de 1000 s es cerca de 0.02.

Para explicar este fenómeno, se mide la fracción de desintegraciones causadas por invalidaciones de grupo y aislamiento de cabezas. Dichas mediciones se muestran en la figura 4.3(b), en la que se puede observar que la mayoría de las desintegraciones para redes de 25 y 50 nodos se deben al aislamiento de la cabeza de grupo. La razón de esto es que los grupos formados fuera de las áreas populares se ven afectados por la escasez de conectividad de la red, producto del área de cobertura inalámbrica reducida de cada terminal. Esta situación se revierte cuando el tamaño de la red es mayor que 50 nodos ya que, con el aumento de este parámetro, también aumenta la cantidad de grupos adyacentes, especialmente en zonas populares. Por esta razón, la probabilidad de desintegración de grupo por invalidación se incrementa, ya que mientras mayor es el número de grupos adyacentes, mayor es la probabilidad de que las cabezas de grupo dejen de cumplir con la política de validez que corresponda.

Con base en esta evidencia, es posible enunciar que el nivel de estabilidad de los grupos depende en buena medida de la distribución espacial de los puntos de recorrido y de las características de la movilidad de los nodos. Por esta razón, los criterios de elección no muestran las ventajas que pueden ser observadas empleando otros modelos de movilidad que no están diseñados para representar las características de la movilidad humana, como RWP y RW.

A diferencia del criterio de elección de cabeza de grupo, los parámetros  $k$ ,  $i$  y  $d$  sí afectan la estabilidad de los grupos, como se muestra en la figura 4.4. Por esta razón, a partir de este punto sólo se explican los resultados de desempeño obtenidos de aplicar el criterio del grado máximo porque son representativos de las configuraciones con otros criterios de elección. Los resultados mostrados en la figura son obtenidos de una red de 300 nodos y tienen barras de error con un nivel de confianza del 95 %.

Específicamente, en la figura 4.4(a) es posible notar lo siguiente:

1. El ancho de las barras de error mostradas en la figura 4.4(a) decrece conforme aumenta el tamaño de la red. Esto se debe a que en los escenarios con tamaños de red mayores que 50 nodos existe una mayor cantidad de grupos que en los casos anteriores, por lo que en tales escenarios se incrementa la cantidad de invalidaciones de grupos y, por lo tanto, se obtienen más mediciones.
2. La ganancia en estabilidad producto de incrementar el radio de agrupamiento de uno

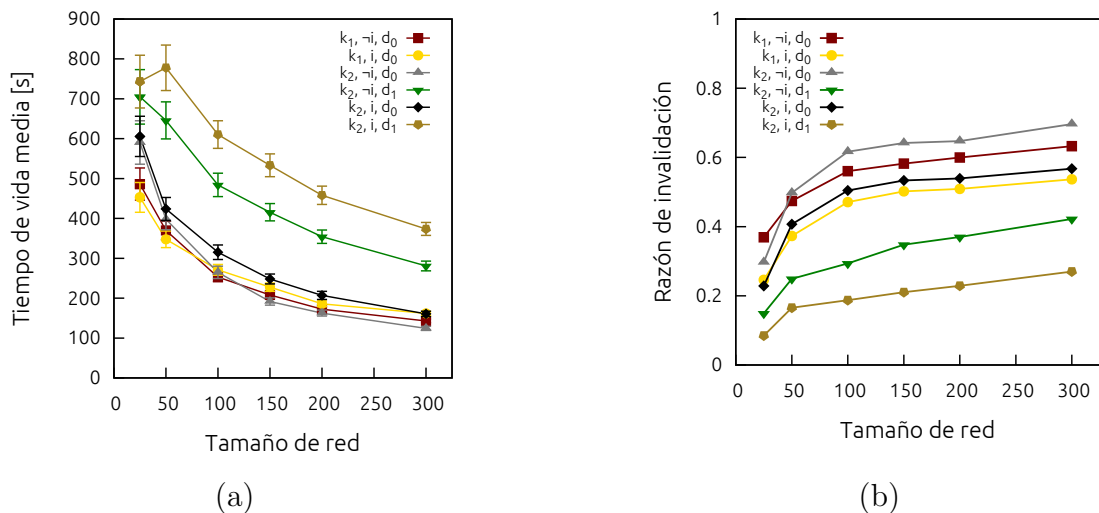


Figura 4.4: Nivel de estabilidad de distintas políticas de validez. (a) Tiempo de vida promedio de los grupos empleando distintas políticas de validez. (b) Razón de desintegración debida a invalidaciones.

a dos saltos bajo la política estricta (configuraciones con parámetros  $-i$  y  $d_0$ ) se pierde a partir de redes de tamaño mayor que 100 nodos. De hecho, la configuración complementaria, es decir la de parámetros  $k_1$ ,  $-i$  y  $d_1$ , da un rendimiento ligeramente mayor que la de  $k_2$  después de tal tamaño.

3. La política de delegación de rol da un mayor nivel de estabilidad en grupos de radio dos que en grupos de radio uno. Esto se debe a que los grupos de radio dos se componen por más nodos que su contraparte, en consecuencia, las cabezas de grupo tienen más opciones para delegar su rol y el tiempo de vida de los grupos puede alargarse. No obstante, la ganancia en el nivel de estabilidad dada por las configuraciones con parámetros  $k_2$ ,  $i$  y  $d_0$  decrece conforme aumenta el tamaño de la red. Esto indica que, aun con esta configuración, se sigue teniendo el problema del número de grupos adyacentes, esto porque la acción de delegar el rol no libera al grupo de los posibles conflictos con los que están de los alrededores.
4. La política flexible (configuraciones con parámetro  $d_1$ ) aumenta considerablemente el nivel de estabilidad exhibido por los grupos. Esto se debe a que la política permite que los grupos toleren a los adyacentes, permitiendo que las cabezas de grupo se acerquen hasta un salto de distancia. Esta medida hace que la red jerárquica sea lo suficientemente flexible para ser establecida en redes móviles.
5. La política de delegación de rol y la flexible dan el mayor nivel de estabilidad en todos los casos, como muestra la curva con parámetros de configuración  $k_2$ ,  $i$  y  $d_1$ . En efecto, la curva muestra que el tiempo de vida promedio de los grupos formados en una red de 300 nodos es aproximadamente de 400 s, al menos 200 segundos más que el tiempo de vida dado por las configuraciones con parámetro  $d_0$ .

En la figura 4.4(b), se ilustra la razón de desintegración por invalidación de grupo. Ahí es

posible observar que, al igual que con los criterios de elección de cabeza de grupo, la razón de desintegraciones por invalidación aumenta conforme aumenta el tamaño de la red. La figura también muestra que la razón de invalidaciones es menor que 0.4 con la política flexible en todos los casos. De hecho, este rendimiento es mejorado si se emplea la política de delegación de rol en conjunto con la de flexibilidad, obteniéndose una razón de desintegración menor que 0.27, aproximadamente, en todos los casos. Además, la figura 4.4(b) muestra que el peor caso corresponde a la configuración con parámetros de configuración  $k_2$ ,  $\neg i$  y  $d_0$ . Esto significa que reducir el número de grupos mediante el incremento del radio de agrupamiento no es buena estrategia para mejorar el nivel de estabilidad de las redes jerárquicas.

### 4.3.3. Costo del mantenimiento de la red jerárquica

El número de reafiliaciones por segundo se muestra en las figuras 4.5(a) y (b). Específicamente, en la primera se muestran las reafiliaciones debidas a la movilidad de los miembros y en la segunda las debidas a las desintegraciones de grupo. En ambas figuras, se puede notar que mientras el tamaño de la red es más grande, el número de reafiliaciones por segundo es mayor.

De acuerdo con la figura 4.5(a), las reafiliaciones debidas a la movilidad de los miembros tienden a crecer más rápido que las debidas a desintegraciones. Claramente, la tendencia mostrada en esta figura tiene que ver con el aumento en el número de grupos explicado en el apartado 4.3.1. Además, es posible deducir que este fenómeno ocurre con mayor intensidad en las áreas populares, donde los nodos tienen la oportunidad de unirse a varios grupos durante su viaje.

Los efectos de las políticas de validez en el costo del mantenimiento de la red jerárquica se presentan en la figura 4.5(b). Estos resultados muestran que la política estricta aplicada a

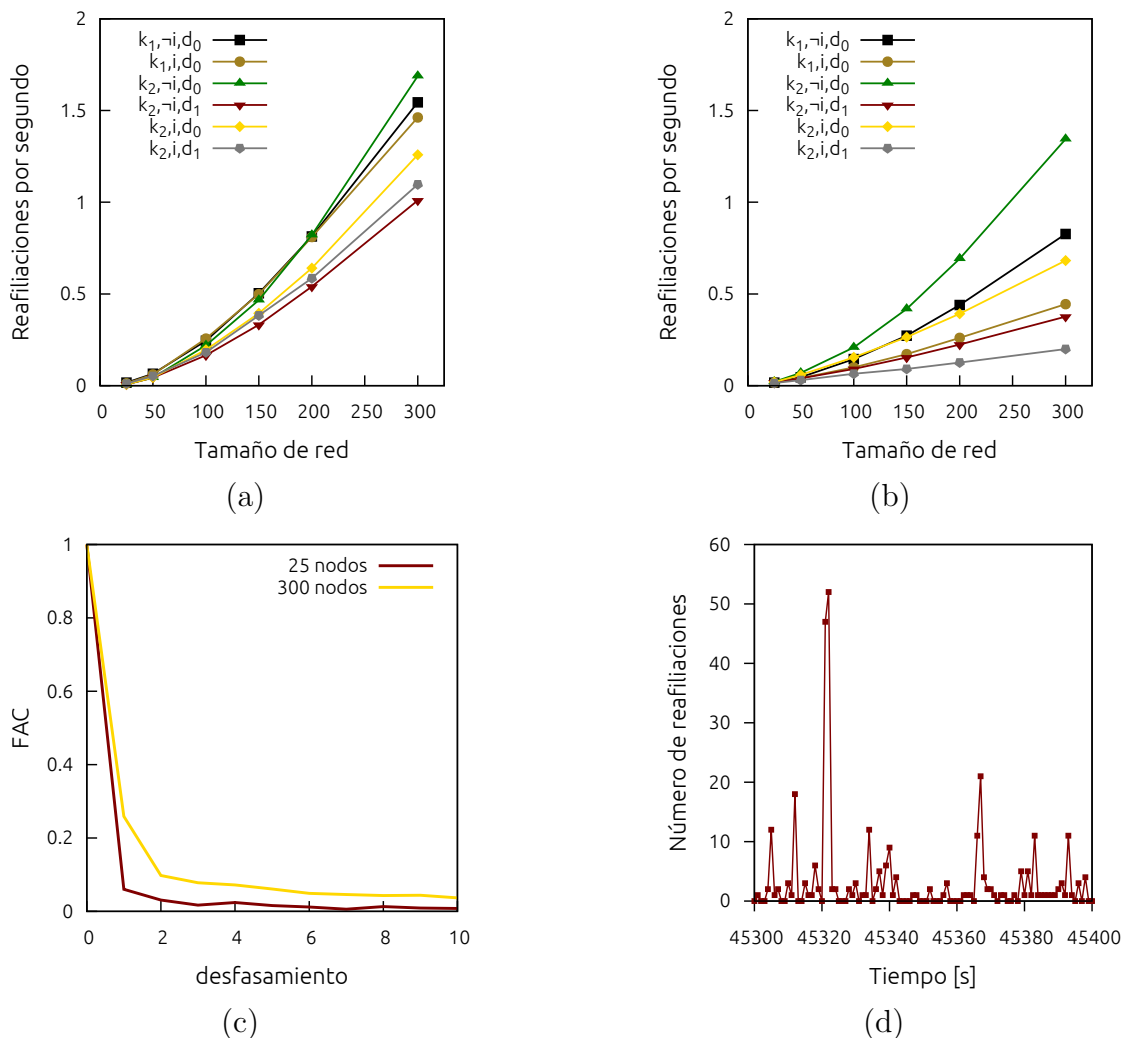


Figura 4.5: Costo del mantenimiento de redes jerárquicas construidas por diferentes políticas de validez. (a) Tasa de reafiliaciones promedio debida a la movilidad de los miembros. (b) Tasa de reafiliaciones promedio por invalidaciones de grupos por política estricta. (c) Función de autocorrelación (FAC) del número de reafiliaciones. (d) Traza del número de reafiliaciones producidas en una red de 300 nodos bajo la configuración antes mencionada.

grupos de radio dos produce el mayor costo de mantenimiento debido al número de invalidaciones que se producen bajo tales configuraciones. Por esta razón, se reafirma la necesidad de incorporar políticas flexibles para reducir el costo del mantenimiento cuando se aumenta el radio de los grupos. Esto se soporta por los resultados que corresponden a las configuraciones en las que se aplica la política de flexibilidad (configuraciones con parámetro  $d_1$ ), las

cuales exhiben las tasas de reafiliación más bajas. De hecho, de acuerdo con la figura 4.5(b) la diferencia entre la peor configuración y la mejor es de 1.14 reafiliaciones por segundo, aproximadamente, para el caso más extremo que corresponde a la red de 300 nodos.

Con base en la probabilidad de que los grupos se compongan por un número de nodos considerable y en los resultados explicados arriba, es posible notar que las cabezas de grupo pueden convertirse en cuellos de botella debido a la cantidad de trabajo que potencialmente tendrían que despachar. Para ilustrar esto, en la figura 4.5(c) se muestra la función de autocorrelación de la tasa de reafiliaciones observada en una red de 25 y una de 300 nodos donde se aplica la configuración con parámetros  $\langle \text{max grado}, k_2, -i, d_0 \rangle$ . El decaimiento lento que exhiben las funciones de autocorrelación implica que las reafiliaciones pueden ocurrir en ráfagas, es decir, en condiciones normales las cabezas de grupo tienen que servir sólo una pequeña tasa de reafiliaciones por segundo, como se observa en las figuras 4.5(a) y (b). No obstante, cuando se dispara un proceso de reorganización debido a la invalidación de un grupo, los miembros deben afiliarse a un nuevo líder, lo que produce un número significativo de reafiliaciones a atender. Consecuentemente, el servicio provisto por las cabezas de grupo puede denegarse temporalmente mientras la red jerárquica se repara. En adición, este proceso puede interferir las comunicaciones del área donde la red está siendo reparada.

Un caso donde la cabeza de grupo deba de afiliar a un número considerable de miembros se muestra en la serie de tiempo ilustrada en la figura 4.5(d). La serie muestra un período de actividad intenso experimentado por una red de 300 nodos bajo la configuración  $\langle \text{maxgrado}, k_2, -i, d_0 \rangle$ . En la serie, es posible notar que los *picos* altos son precedidos por otros poco menores a ellos, lo que significa que la desintegración de un grupo puede causar la desintegración de otros más grandes. La serie también muestra que el número de reafiliaciones decrece después de haber ocurrido un gran número de éstas. Esto sugiere que los grupos no se invalidan progresivamente debido a que no están totalmente conectados entre sí ya que se

crean en áreas confinadas que pueden estar geográficamente separadas entre sí. Consecuentemente, se vuelve poco probable que todos los grupos puedan desintegrarse por la invalidación de uno. Este es otro fenómeno que no puede ser apreciado en evaluaciones donde se emplean modelos de movilidad que no consideran las características de la movilidad humana y donde las terminales tienen un área de cobertura grande asignada para evitar particiones de red.

## **4.4. Discusión**

Con base en los resultados obtenidos de evaluar las distintas estrategias estabilizantes presentadas en este capítulo, se pueden establecer las siguientes bases para el desarrollo de servicios de búsqueda provistos por una red jerárquica. En la literatura, se han presentado distintos criterios de elección de líder para aumentar la estabilidad de la red. No obstante, los criterios evaluados en este trabajo no muestran diferencias de desempeño significativas entre sí, inclusive en el caso de los que se propusieron para estabilizar redes jerárquicas en las que algunas propiedades de la movilidad humana se toman en cuenta. Esto muestra que las soluciones diseñadas para ambientes genéricos o no detallados no necesariamente operan correctamente al considerarse escenarios más apegados a la realidad. Por ello, es necesario tener en cuenta el mayor número de elementos que modelen el escenario donde la solución va a ser aplicada, esto para dar mayor garantía de su éxito.

Otra cuestión a considerar es que la probabilidad de que los grupos exhiban tiempos de vida largos es pequeña. Para solventar esta cuestión, en áreas confinadas con baja popularidad puede aplicarse una política preventiva de delegación de rol que evite desintegraciones por aislamiento, esto para cubrir el caso en que la cabeza de grupo sale de su área. Para aplicarla, los líderes cederían sus responsabilidades después de cierto tiempo que puede ser calibrado con base en el tamaño de su grupo y en la distribución del tiempo de pausa. En el caso de las



áreas populares, se puede establecer una política que force a las cabezas de grupo a heredar su rol una vez que están a cierta distancia de una vecina y no hasta que sean vecinas locales. Para ofrecer cierta garantía en la duración de los enlaces lógicos entre los líderes al aplicar esta medida, la distancia entre los ellos puede basarse en los resultados de la duración de ruta presentados en la sección 3.3.2.

Finalmente, es importante disminuir la razón de afiliaciones debido a que ésta tiende a crecer conforme aumenta el tamaño de la red. Para atender esta cuestión, puede definirse una política de actualización de estado *perezosa*, en la que las cabezas de grupo afilien a los nodos cada que se requiera o después de intervalos de tiempo un tanto largos. Esto podría operar bien para prestar el servicio de búsqueda ya que sólo se requiere conocer a los miembros de grupo que potencialmente puedan prestar recursos. Además, esta política también aliviaría el problema de los grupos numerosos, ya que sólo se mantendrían los enlaces de los miembros que requiere el servicio para operar.



# Capítulo 5

## Conclusiones y perspectivas

Con el objetivo de sentar las bases para el desarrollo de servicios eficientes de búsqueda para redes ad hoc móviles, en esta tesis se determinaron las estrategias que hacen que las tablas *hash* distribuidas puedan funcionar en ambientes donde la topología lógica es dinámica. Además, se presentó un análisis de las características estadísticas de las MANET en las que el movimiento de los nodos sigue patrones de movilidad humana. Finalmente, se determinaron distintas estrategias estabilizantes que permiten que las redes lógicas basadas en grupos preserven su organización tanto como sea posible.

Para ilustrar la utilidad de los resultados mostrados en esta tesis doctoral, enseguida presentamos una discusión de cómo aprovecharlos en la construcción de servicios de búsqueda eficientes para redes ad hoc móviles.

## 5.1. Bases para el diseño de un servicio de búsqueda P2P eficiente

Se define como servicio de búsqueda al conjunto de protocolos que soportan la resolución de peticiones por recursos que se encuentran distribuidos en una red P2P. El servicio de búsqueda recibe por entrada el identificador único del recurso solicitado y regresa como resultado el identificador único de los participantes que poseen el recurso solicitado.

Como se menciona en el capítulo 1, el servicio de búsqueda puede basarse en técnicas de búsqueda no estructurada, jerárquica y estructurada. De estas tres opciones, las dos últimas resultan ser las más eficientes para resolver consultas. No obstante, estos servicios se construyen sobre redes lógicas cuyo costo de mantenimiento puede ser prohibitivo si la topología física de la red cambia abruptamente con respecto al tiempo. En este trabajo de investigación, se muestra que construir una red lógica sobre una red ad hoc móvil es factible ya que los resultados presentados en el capítulo 3 indican que la conectividad que exhibe la red y el tiempo de vida de las rutas multisalto es suficiente para establecer enlaces lógicos duraderos. En el caso promedio, un enlace lógico establecido entre un par de nodos separados por una distancia de seis saltos exhibiría un tiempo de vida aproximado de 5 cinco minutos. Esto indica que no es necesario enviar mensajes de control a una frecuencia alta para mantener correctos los enlaces de la red lógica.

Los resultados presentados en este trabajo también dan indicios de las estrategias a seguir para mantener actualizado el estado de los participantes de la red P2P y qué estrategias aplicar para realizar la búsqueda de recursos. Teniendo como base el tiempo de vida de las rutas multisalto y el análisis de los resultados obtenidos de la evaluación de desempeño de las tablas *hash* distribuidas, el estado de los pares puede actualizarse con el tráfico de red. Para ello, las consultas por recursos también deben contener información de control dentro

del mismo mensaje que sirva para actualizar las entradas de las tablas de encaminamiento y las estructuras donde se almacenan las referencias a los recursos compartidos. Aplicando esta estrategia, las entradas incorrectas en el estado de los participantes se reparan hasta que sean detectadas, ya que, en teoría, su número debe ser pequeño dado que se aprovecha el tráfico de red para enviar mensajes de mantenimiento. A su vez, los resultados indican que el estado de los participantes puede mantenerse siguiendo una estrategia *soft state*, es decir, las entradas del estado pueden eliminarse después de un cierto período de tiempo que es función de la distancia hacia algún nodo (ver figura 3.6(b)). Por ejemplo, las entradas no usadas que corresponden a vecinos locales pueden conservarse en promedio 20 minutos y las entradas no usadas de vecinos a dos saltos pueden descartarse después de 13 minutos, aproximadamente.

Del análisis de la estabilidad de estrategias de agrupamiento se deduce que no es buena táctica el hacer que las cabezas de grupo actualicen su estado cada vez que un miembro cambia su afiliación. De acuerdo con los resultados de desempeño mostrados en el capítulo 4, el número de reafiliaciones debidas a la movilidad es muy alto, por lo que aplicar dicha estrategia resultaría muy costoso. En lugar de ello, pueden aplicarse políticas de reafiliación *perezosa*. Además, en este análisis se mostró que el criterio de elección de cabeza de grupo no afecta el nivel de estabilidad de la red, por lo que la elección puede realizarse empleando un criterio de cómputo simple, p. ej., el grado de los nodos. Finalmente, se observó que el tiempo de vida de los grupos puede ser extendido si se consideran políticas de validez flexibles.

Con respecto a las estrategias para realizar la búsqueda, los resultados reportados en esta tesis doctoral indican que es en extremo importante considerar que los nodos se mueven en todo momento. De no tenerse en cuenta este detalle, el establecimiento de la red lógica será incorrecto y, por lo tanto, las búsquedas van a fallar en servicios de búsqueda jerárquicos y estructurados. Otro punto importante es que la red lógica debe diseñarse para explotar la conectividad que las redes ad hoc móviles exhiben cuando se considera la movilidad humana.

Para ello, la red lógica debe permitir que la comunicación entre nodos fuente y nodos destino no dependa únicamente de un conjunto de nodos intermedios sobre los que se establezca una ruta multisalto, sino que debe proveer rutas alternas siempre que sea posible.

## 5.2. Líneas de investigación

La primera línea de investigación que deja este trabajo es el diseño de un servicio de búsqueda basado en una tabla *hash* distribuida. Esta decisión está fundamentada en el hecho de que la conectividad de la red podría explotarse de mejor manera con el enfoque estructurado. Además, la búsqueda estructurada no presenta puntos únicos de falla porque, a diferencia del enfoque jerárquico, no delega funciones especiales a un conjunto específico de nodos. En adición, de acuerdo con los resultados mostrados en el capítulo 4, las cabezas de grupo que se encuentren dentro de áreas populares pueden volverse cuellos de botella debido a la gran cantidad de miembros que tendrían que servir.

Aparte del servicio de búsqueda, una aplicación P2P requiere de un servicio de descarga para operar, el cual también puede basarse en el conocimiento presentado en esta tesis doctoral. Se define como *servicio de descarga* al conjunto de protocolos que soportan la transferencia de datos entre los prestadores de recursos y los solicitantes. Cuando los recursos compartidos en la red P2P son ciclos de procesamiento, almacenamiento, un geolocalizador o algún sensor, el servicio de descarga no requiere ser muy sofisticado ya que, generalmente, los prestadores sólo requieren enviar un archivo pequeño a los solicitantes para servir una petición. No obstante, un servicio de descarga simple no es factible para la transmisión de un volumen considerable de datos ya que, dependiendo del caudal de datos de la red, el tiempo de vida de los enlaces lógicos puede ser insuficiente para transmitir archivos de cierto tamaño, por lo que surge la necesidad de diseñar un servicio de descarga sofisticado, especialmente cuando la distancia

entre los proveedores y los solicitantes no es pequeña.

Generalmente, en las redes P2P con infraestructura se emplean los protocolos HTTP, FTP y BitTorrent para transferir un archivo a un solicitante. Sin embargo, estos protocolos no pueden ser empleados directamente en las redes ad hoc móviles porque, al igual que los protocolos de búsqueda, no están diseñados para trabajar en un ambiente donde la infraestructura de red es móvil. En la literatura, se han propuesto distintos protocolos de descarga para redes ad hoc móviles, p. ej., ORION [17] para transferencias punto a punto, IRA [78] para transferencias de archivos siguiendo el paradigma de encaminamiento oportunista y distintas adaptaciones [74, 102, 103] del protocolo BitTorrent. En dichos artículos, la descarga de contenidos se presenta como un problema muy complicado de manejar, sin embargo, el problema ha sido poco observado desde el punto de vista de la movilidad humana. Por ello, resultaría de mucho interés el desarrollo de un servicio de descarga para redes ad hoc móviles que explotara las características estadísticas del movimiento humano.

La última línea de investigación que deja este trabajo es el desarrollo de aplicaciones P2P para redes ad hoc móviles. Del hecho de que las redes ad hoc móviles presentan un caudal de datos bajo, naturalmente surge la necesidad de definir el tipo de aplicaciones que efectivamente pueden proveerse con esta infraestructura de red. La importancia de atender esta cuestión radica en el hecho de que, en definitiva, el despliegue real de redes ad hoc móviles depende del desarrollo de aplicaciones atractivas para los usuarios.





# Referencias bibliográficas

- [1] Marco Conti y Silvia Giordano. Multihop ad hoc networking: The reality. *IEEE Communications Magazine*, 45(4):88–95, abril 2007.
- [2] Marco Conti y Silvia Giordano. Multihop ad hoc networking: The theory. *IEEE Communications Magazine*, 45(4):78–86, abril 2007.
- [3] Shahbaz Akhtar Abid, Mazliza Othman, y Nadir Shah. A survey on DHT-based routing for large-scale mobile ad hoc networks. *ACM Computer Surveys*, 47(2):20:1–20:46, agosto 2014.
- [4] Marcel C. Castro, Andreas J. Kessler, Carla-Fabiana Chiasserini, Claudio Casetti, y Ibrahim Korpeoglu. Peer-to-peer overlay in mobile ad-hoc networks. En *Handbook of Peer-to-Peer Networking*, páginas 1045–1080. Springer US, Boston, EUA, 2010.
- [5] Himabindu Pucha, Y. Charlie Hu, y M. Das Saumitra. Peer-to-Peer overlay abstractions in MANETs. En *Handbook on Theoretical and Algorithmic Aspects of Sensor, Ad Hoc Wireless, and Peer-to-Peer Networks*, capítulo 47, páginas 857–874. Springer US, Boston, EUA, 2005.
- [6] Ralf Steinmetz y Klaus Wehrle. What is this? En *Peer-to-Peer Systems and Applications*, capítulo 2, páginas 9–16. Springer-Verlag, Berlin Heidelberg, 2005.

- [7] Gunnar Kreitz y Fredrick Niemela. Spotify – large scale, low latency, p2p music-on-demand streaming. En *IEEE Tenth International Conference on Peer-to-Peer Computing (IEEE P2P)*, páginas 1–10, Delft, Países Bajos, agosto 2010.
- [8] Salman A. Baset y Henning G. Schulzrinne. An analysis of the Skype peer-to-peer internet telephony protocol. En *Proceedings of the 25th IEEE International Conference on Computer Communications (INFOCOM)*, páginas 1–11, Barcelona, España, abril 2006.
- [9] What is the bittorrent protocol? <http://tinyurl.com/o7x8haf>, septiembre 2015. Accedido el 22/09/2015.
- [10] Elena Meshkova, Janne Riihijärvi, Marina Petrova, y Petri Mähönen. A survey on resource discovery mechanisms, peer-to-peer and service discovery frameworks. *Computer Networks*, 52(11):2097–2128, agosto 2008.
- [11] Patrick Kirk. What is gnutella? <http://tinyurl.com/omwg8jo> (Accedido: 15/09/2015), 2003.
- [12] Ion Stoica, Robert Morris, David Liben-Nowell, David R. Karger, M. Frans Kaashoek, Frank Dabek, y Hari Balakrishnan. Chord: A scalable peer-to-peer lookup protocol for internet applications. *IEEE/ACM Transactions on Networking*, 11(1):17–32, febrero 2003.
- [13] Petar Maymounkov y David Mazières. Kademia: A peer-to-peer information system based on the XOR metric. En *Revised Papers from the First International Workshop on Peer-to-Peer Systems (IPTPS)*, páginas 53–65, Cambridge, EUA, marzo 2002.
- [14] Raphael Manfredi Tor Klingberg. Gnutella 0.6. draft, junio 2002.

- [15] Piyush Gupta y P. R. Kumar. The capacity of wireless networks. *IEEE Transactions on Information Theory*, 46(2):388–404, marzo 2000.
- [16] Daniel Stutzbach y Reza Rejaie. Understanding churn in peer-to-peer networks. En *Proceedings of the 6th ACM SIGCOMM Conference on Internet Measurement (IMC)*, páginas 189–202, Río de Janeiro, Brasil, octubre 2006.
- [17] Alexander Klemm, Christoph Lindemann, y Oliver P. Waldhorst. A special-purpose peer-to-peer file sharing system for mobile ad hoc networks. En *Proceedings of the 58th IEEE Vehicular Technology Conference (VTC-Fall)*, páginas 2758–2763, Orlando, EUA, octubre 2003.
- [18] Ingo Gruber, Rüdiger Schollmeier, y Wolfgang Kellerer. Performance evaluation of the mobile peer-to-peer service. En *IEEE International Symposium on Cluster Computing and the Grid (CCGrid)*, páginas 363–371, 2004.
- [19] Marco Conti, Enrico Gregori, y Giovanni Turi. A cross-layer optimization of gnutella for mobile ad hoc networks. En *Proceedings of the 6th Acm International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc)*, páginas 343–354, Chicago, EUA, mayo 2005.
- [20] Himabindu Pucha, Saumitra M. Das, y Y. Charlie Hu. Ekta: An efficient DHT substrate for distributed applications in mobile ad hoc networks. En *Proceedings of the Sixth IEEE Workshop on Mobile Computing Systems and Applications (WMCSA)*, páginas 163–173, English Lake District, Reino Unido, diciembre 2004.
- [21] T. Zahn y J. Schiller. Madpastry: A DHT substrate for practicably sized MANETs. En *5th Workshop on Applications and Services in Wireless Networks (ASWN)*, 2005.
- [22] Matthew Caesar, Miguel Castro, Edmund B. Nightingale, Greg O’Shea, y Antony

- Rowstron. Virtual ring routing: Network routing inspired by DHTs. *SIGCOMM Computer Communication Review*, 36(4):351–362, agosto 2006.
- [23] Jakob Eriksson, Michalis Faloutsos, y Srikanth V. Krishnamurthy. DART: dynamic address routing for scalable ad hoc and mesh networks. *IEEE/ACM Transactions on Networking*, 15(1):119–132, febrero 2007.
- [24] Jose J. Garcia-Luna-Aceves y Dhananjay Sampath. Scalable integrated routing using prefix labels and distributed hash tables for MANETs. En *Proceedings of the IEEE 6th International Conference on Mobile Adhoc and Sensor Systems (MASS)*, páginas 188–198, Macao, China, octubre 2009.
- [25] Marcello Caleffi y Luigi Paura. M-DART: multi-path dynamic address routing. *Wireless Communications and Mobile Computing*, 11(3):392–409, 2011.
- [26] Nadir Shah, Depei Qian, y Rui Wang. MANET adaptive structured P2P overlay. *Peer-to-Peer Networking and Applications*, 5(2):143–160, 2012.
- [27] Rumi Ghosh y Jose J. Garcia-Luna-Aceves. Automatic incremental routing using multiple roots. En *IEEE 32nd International Performance Computing and Communications Conference (IPCCC)*, páginas 1–9, San Diego, EUA, diciembre 2013.
- [28] Adnan Noor Mian, Roberto Baldoni, y Roberto Beraldi. A survey of service discovery protocols in multihop mobile ad hoc networks. *IEEE Pervasive Computing*, 8(1):66–74, marzo 2009.
- [29] Yogesh Chaba, Yudhvir Singh, y Manish Joon. Performance evaluation and analysis of cluster based routing protocols in MANETs. En *International Conference on Advances in Computing, Control, Telecommunication Technologies (ACT)*, páginas 64–66, Trivandrum, India, diciembre 2009.

- [30] Liliana Enciso Quispe y Luis Mengual Galán. Behavior of ad hoc routing protocols, analyzed for emergency and rescue scenarios, on a real urban area. *Expert Systems with Applications*, 41(5):2565–2573, abril 2014.
- [31] Jane Y. Yu y Peter H.J. Chong. A survey of clustering schemes for mobile ad hoc networks. *IEEE Communications Surveys & Tutorials*, 7(1):32–48, First 2005.
- [32] Kyunghan Lee, Seongik Hong, Seong Joon Kim, Injong Rhee, y Song Chong. SLAW: self-similar least-action human walk. *IEEE/ACM Transactions on Networking*, 20(2):515–529, abril 2012.
- [33] Marta C. González, César A. Hidalgo, y Albert-László Barabási. Understanding individual human mobility patterns. *Nature*, 453(7196):779–782, junio 2008.
- [34] Injong Rhee, Minsu Shin, Seongik Hong, Kyunghan Lee, Seong Joon Kim, y Song Chong. On the levy-walk nature of human mobility. *IEEE/ACM Transactions on Networking*, 19(3):630–643, junio 2011.
- [35] Thomas Karagiannis, Jean-Yves Le Boudec, y Milan Vojnović. Power law and exponential decay of intercontact times between mobile devices. *IEEE Transactions on Mobile Computing*, 9(10):1377–1390, octubre 2010.
- [36] Arta Doci, Georgios Samakovitis, y Vijaya Raju. Impact of mobility in ad hoc protocol design. En *World Congress on Computer Science and Information Engineering (WRI)*, páginas 38–43, Los Ángeles, EUA, marzo 2009.
- [37] Vincent Lenders, Jörg Wagner, y Martin May. Analyzing the impact of mobility in ad hoc networks. En *Proceedings of the 2nd International Workshop on Multi-hop Ad Hoc Networks: From Theory to Reality (REALMAN)*, páginas 39–46, Florencia, Italia, mayo 2006.

- [38] Fahim Maan y Nauman Mazhar. MANET routing protocols vs mobility models: A performance evaluation. En *Third International Conference on Ubiquitous and Future Networks (ICUFN)*, páginas 179–184, Dalian, China, junio 2011.
- [39] Adán G. Medrano-Chávez, Elizabeth Pérez-Cortés, y Miguel Lopez-Guerrero. Studying the effect of human mobility on manet topology and routing: Friend or foe? En *Proceedings of the 13th ACM International Symposium on Mobility Management and Wireless Access (MobiWac)*, páginas 39–46, Cancún, México, noviembre 2015.
- [40] Adán G. Medrano-Chávez, Elizabeth Pérez-Cortés, y Miguel Lopez-Guerrero. A performance comparison of Chord and Kademia DHTs in high churn scenarios. *Peer-to-Peer Networking and Applications*, 8(5):807–821, junio 2014.
- [41] Adán G. Medrano-Chávez, Elizabeth Pérez-Cortés, y Miguel Lopez-Guerrero. On the effect of peer online times on the lookup service of Chord and Kademia P2P systems. En *IEEE Latin-America Conference on Communications (LATINCOM)*, páginas 1–6, Santiago, Chile, noviembre 2013.
- [42] INET framework. <http://inet.omnetpp.org/>. Accedido el 2015/02/15.
- [43] Andrés Varga y Rudolf Hornig. An overview of the OMNeT++ simulation environment. En *Proceedings of the 1st International Conference on Simulation Tools and Techniques for Communications, Networks and Systems & Workshops (SIMUtools)*, páginas 1–10, Marsella, Francia, marzo 2008.
- [44] Adán G. Medrano-Chávez. Evaluación de la confiabilidad de índices P2P en presencia de alta transitoriedad. Tesis de maestría (Universidad Autónoma Metropolitana, Ciudad de México), octubre 2011.
- [45] Donald E. Eastlake y Paul E. Jones. US secure hash algorithm 1 (SHA1). Technical Report FIPS 180-1, U.S. Department of Commerce/NIST, Springfield, EUA, abril 1995.

- [46] Sean Rhea, Dennis Geels, Timothy Roscoe, y John Kubiatowicz. Handling churn in a DHT. En *Proceedings of the Annual Conference on Usenix Annual Technical Conference (USENIX)*, páginas 1–14, Boston, EUA, noviembre 2004.
- [47] Supriya Krishnamurthy, Sameh El-Ansary, Erik Aurell, y Seif Haridi. An analytical study of a structured overlay in the presence of dynamic membership. *IEEE/ACM Transactions on Networking*, 16(4):814–825, agosto 2008.
- [48] Zhiyu Liu, Ruifeng Yuan, Zhenhua Li, Hongxing Li, y Guihai Chen. Survive under high churn in structured P2P systems: Evaluation and strategy. En *Proceedings of the 6th International Conference on Computational Science (ICCS)*, páginas 404–411, Reading, Reino Unido, mayo 2006.
- [49] Krishna P. Gummadi, Ramakrishna Gummadi, Steven D. Gribble, Sylvia Ratnasamy, Scott Shenker, y Ion Stoica. The impact of DHT routing geometry on resilience and proximity. En *Proceedings of the Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications (ACM SIGCOMM)*, páginas 381–394, Karlsruhe, Alemania, agosto 2003.
- [50] Joseph S. Kong, Jesse S. A. Bridgewater, y Vwani P. Roychowdhury. Resilience of structured P2P systems under churn: The reachable component method. *Computer Communications*, 31(10):2109–2123, junio 2008.
- [51] Jinyang Li, Jeremy Stribling, Thomer M. Gil, Robert Morris, y M. Frans Kaashoek. Comparing the performance of distributed hash tables under churn. En *Proceedings of the Third International Conference on Peer-to-Peer Systems (IPTPS)*, páginas 87–99, La Jolla, EUA, febrero 2004.
- [52] Zhonghong Ou, Erkki Harjula, y Mika Ylianttila. Effects of different churn models on the performance of structured peer-to-peer networks. En *Proceedings of the IEEE*

*20th International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*, páginas 2856–2860, Tokio, Japón, septiembre 2009.

- [53] Zhongmei Yao y D. Loguinov. Analysis of link lifetimes and neighbor selection in switching DHTs. *IEEE Transactions on Parallel and Distributed Systems*, 22(11):1834–1841, noviembre 2011.
- [54] Octavio Herrera y Taieb Znati. Modeling churn in P2P networks. En *Proceedings of the 40th Annual Simulation Symposium (ANSS)*, páginas 33–40, Norfolk, EUA, marzo 2007.
- [55] Suvadip Batabyal y Parama Bhaumik. Mobility models, traces and impact of mobility on opportunistic routing algorithms: A survey. *IEEE Communications Surveys & Tutorials*, PP(99), 2015.
- [56] Joanne Treurniet. A taxonomy and survey of microscopic mobility models from the mobile networking domain. *ACM Computing Surveys*, 47(1):14–32, julio 2014.
- [57] Tracy Camp, Jeff Boleng, y Vanessa Davies. A survey of mobility models for ad hoc network research. *Wireless Communications and Mobile Computing*, 2(5):483–502, septiembre 2002.
- [58] Fan Bai, Narayanan Sadagopan, Bashkar Krishnamachari, y Ahmed Helmy. Modeling path duration distributions in MANETs and their impact on reactive routing protocols. *IEEE Journal on Selected Areas in Communications*, 22(7):1357–1373, septiembre 2004.
- [59] Michael Pascoe, Javier Gomez, Victor Rangel, y Miguel Lopez-Guerrero. Route duration modeling for mobile ad hoc networks. *Wireless Networks*, 16(3):743–757, abril 2010.



- [60] Shyh-En Lin, Wan-Ping Tsai, Meng-Hsun Tsai, y Ai-Chun Pang. IROL: A humanoid mobility model for mobile ad hoc network. En *IEEE International Conference on Communications (ICC)*, páginas 2496–2501, Sídney, Australia, junio 2014.
- [61] Gurkan Solmaz, Mustapha I. Akbas, y Damla Turgut. A mobility model of theme park visitors. *IEEE Transactions on Mobile Computing*, PP(99), 2015.
- [62] Zhe Luo, Ying Cui, Xinbing Wang, y Hanwen Luo. On the throughput and delay in ad hoc networks with human mobility. *IEEE Transactions on Communications*, 63(6):2273–2287, junio 2015.
- [63] Josh Broch, David A. Maltz, David B. Johnson, Yih-Chun Hu, y Jorjeta Jetcheva. A performance comparison of multi-hop wireless ad hoc network routing protocols. En *Proceedings of the 4th Annual ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom)*, páginas 85–97, Dallas, EUA, octubre 1998.
- [64] Aarti Munjal, Tracy Camp, y William C. Navidi. SMOOTH: A simple way to model human mobility. En *Proceedings of the 14th ACM International Conference on Modeling, Analysis and Simulation of Wireless and Mobile Systems (MSWiM)*, páginas 351–360, Miami, EUA, octubre 2011.
- [65] Jungkeun Yoon, Mingyan Liu, y Brian Noble. Random waypoint considered harmful. En *Twenty-Second Annual Joint Conference of the IEEE Computer and Communications (INFOCOM)*, volume 2, páginas 1312–1321, San Francisco, EUA, marzo 2003.
- [66] William C. Navidi y Travy Camp. Stationary distributions for the random waypoint mobility model. *IEEE Transactions on Mobile Computing*, 3(1):99–108, enero 2004.
- [67] Amitava Datta y Subbiah Soundaralakshmi. A survey of state-of-the-art routing protocols for mobile ad hoc networks. En Laurence T. Yang, editor, *Mobile Intelligence*, capítulo 1, páginas 3–25. John Wiley and Sons, Hoboken, EUA, 2010.

- [68] Charles E. Perkins y Elizabeth M. Belding-Royer. Ad-hoc on-demand distance vector routing. En *Proceedings on the Second IEEE Workshop on Mobile Computing Systems and Applications (WMCSA)*, páginas 90–100, Nueva Orleans, EUA, febrero 1999.
- [69] Charles E. Perkins y Elizabeth M. Belding-Royer. Ad hoc on-demand distance vector (AODV) routing. RFC 3561, Network Working Group, julio 2003.
- [70] David B. Johnson, David A. Maltz, y Josh Broch. DSR: the dynamic source routing protocol for multihop wireless ad hoc networks. En *Ad hoc networking*, páginas 139–172. Addison-Wesley Longman Publishing Co., Inc., Boston, EUA, 2001.
- [71] Satish Chandra y Anish Kumar Bharti. Speed distribution curves for pedestrians during walking and crossing. *Procedia - Social and Behavioral Sciences*, 104(0):660–667, 2013.
- [72] Guangyu Pei y Thomas R. Henderson. Validation of OFDM error rate model in ns-3. Technical report, Boeing Research and Technology, Seattle, EUA, 2010.
- [73] Erik Nordström. AODV-UU: An implementation of the AODV routing protocol (IETF RFC 3561). <https://github.com/erimatnor/aodv-uu>. Accedido el 22/09/2015.
- [74] Mohamed Karim Sbai, Emna Salhi, y Chadi Barakat. P2P content sharing in spontaneous multi-hop wireless networks. En *Proceedings of the Second International Conference on Communication Systems and Networks (COMSNETS)*, páginas 1–10, Bangalore, India, enero 2010.
- [75] Christian Tschudin, Per Gunningberg, Henrik Lundgren, y Erik Nordström. Lessons from experimental MANET research. *Ad Hoc Networks*, 3(2):221–233, marzo 2005.
- [76] Aarti Munjal, William C. Navidi, y Tracy Camp. Steady-state of the SLAW mobility model. *Journal of Communications*, 9(4):322–331, abril 2014.

- [77] Suchismita Chinara y Santanu K. Rath. A survey on one-hop clustering algorithms in mobile ad hoc networks. *Journal Network System Management*, 17(1-2):183–207, junio 2009.
- [78] Kang Chen, Haiying Shen, y Haibo Zhang. Leveraging social networks for p2p content-based file sharing in disconnected manets. *IEEE Transactions on Mobile Computing*, 13(2):235–249, febrero 2014.
- [79] Baruch Awerbuch. Complexity of network synchronization. *Journal of the ACM*, 32(4):804–823, octubre 1985.
- [80] Mingliang Jiang, Jinyang Li, y Y. C. Tay. Cluster based routing protocol (CBRP). INTERNET-DRAFT, IETF, agosto 1999.
- [81] Charles E. Perkins y Pravin Bhagwat. Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers. *Computer Communication Review*, 24(4):234–244, octubre 1994.
- [82] Jie Wu, Fei Dai, Ming Gao, y Ivan Stojmenovic. On calculating power-aware connected dominating sets for efficient routing in ad hoc wireless networks. *Journal of Communications and Networks*, 4(1):59–70, marzo 2002.
- [83] Mario Gerla y J. Tzu-chieh Tsai. Multicluster, mobile, multimedia radio network. *Journal of Wireless Networks*, 1:255–265, octubre 1995.
- [84] Prithwish Basu, Naved Khan, y Thomas D. C. Little. A mobility based metric for clustering in mobile ad hoc networks. En *International Conference on Distributed Computing Systems Workshop (CDCS)*, páginas 413–418, Mesa, EUA, abril 2001.
- [85] M.B. Shah, P.P. Verma, S.N. Merchant, y U.B. Desai. Human walk aware mobility resistant efficient clustering for data gathering in cell phone based wireless sensor net-

- works. En *20th Annual Wireless and Optical Communications Conference (WOCC)*, páginas 1–6, Newark, EUA, abril 2011.
- [86] Shivangi Singhal y A. K. Daniel. Cluster head selection protocol under node degree, competence level and goodness factor for mobile ad hoc network using ai technique. En *Proceedings of the 2014 Fourth International Conference on Advanced Computing & Communication Technologies (ACCT)*, páginas 415–420, Rohtak, India, febrero 2014.
- [87] Mainak Chatterjee, SajalK. Das, y Damla Turgut. WCA: A weighted clustering algorithm for mobile ad hoc networks. *Cluster Computing*, 5(2):193–204, abril 2002.
- [88] Mohamed Aissa y Abdelfettah Belghith. Quality of clustering in mobile ad hoc networks. *Procedia Computer Science*, 32:245–252, junio 2014.
- [89] Stefano Basagni. Distributed and mobility-adaptive clustering for multimedia support in multi-hop wireless networks. En *IEEE 50th Vehicular Technology Conference (VTC)*, páginas 889–893 vol.2, Amsterdam, Países Bajos, septiembre 1999.
- [90] Jane Y. Yu y Peter H. J. Chong. 3hBAC (3-hop between adjacent clusterheads): a novel non-overlapping clustering algorithm for mobile ad hoc networks. En *IEEE Pacific Rim Conference on Communications, Computers and signal Processing (PACRIM)*, páginas 318–321 vol.1, Victoria, Canadá, agosto 2003.
- [91] Khac Tiep Mai y Hyunseung Choo. Connectivity-based clustering scheme for mobile ad hoc networks. En *IEEE International Conference on Research, Innovation and Vision for the Future (RIVF)*, páginas 191–197, Ho Chi Minh City, Vietnam, julio 2008.
- [92] Atta Ur Rehman Khan, Shahzad Ali, Saad Mustafa, y Mazliza Othman. Impact of mobility models on clustering based routing protocols in mobile WSNs. En *Proceedings of the 2012 10th International Conference on Frontiers of Information Technology (FIT)*, páginas 366–370, Islamabad, Pakistán, diciembre 2012.

- [93] Aravindhnan Venkateswaran, Venkatesh Sarangan, Natarajan Gautam, y Raj Acharya. Impact of mobility prediction on the temporal stability of MANET clustering algorithms. En *Proceedings of the 2nd ACM International Workshop on Performance Evaluation of Wireless Ad Hoc, Sensor, and Ubiquitous Networks (PE-WASUN)*, páginas 144–151, Quebec, Canadá, octubre 2005.
- [94] William Su, Sung-Ju Lee, y Mario Gerla. Mobility prediction in wireless networks. En *21st Century Military Communications Conference Proceedings (MILCOM)*, páginas 491–495 vol.1, Los Ángeles, EUA, octubre 2000.
- [95] Zainab R. Zaidi, Brian L. Mark, y Roshan K. Thomas. A two-tier representation of node mobility in ad hoc networks. En *First Annual IEEE Communications Society Conference on Sensor and Ad Hoc Communications and Networks (SECON)*, páginas 153–161, Santa Clara, EUA, octubre 2004.
- [96] Anthony Ephremides, Jeffrey E. Wieselthier, y Dennis J. Baker. A design concept for reliable mobile radio networks with frequency hopping signaling. *Proceedings of the IEEE*, 75(1):56–73, enero 1987.
- [97] Geng Chen, Fabián García-Nocetti, Julio Solano-González, y Ivan Stojmenovic. Connectivity based k-hop clustering in wireless networks. En *Proceedings of the 35th Annual Hawaii International Conference on System Sciences (HICSS)*, páginas 2450–2459, Hawaii, EUA, enero 2002.
- [98] Yan Zhang y Jim Mee Ng. A distributed group mobility adaptive clustering algorithm for mobile ad hoc networks. En *IEEE International Conference on Communications (ICC)*, páginas 3161–3165, Pequín, China, mayo 2008.
- [99] Elmano Ramalho Cavalcanti y Marco Aurélio Spohn. Degree of node proximity: A spatial mobility metric for MANETs. En *Proceedings of the 9th ACM International*

- Symposium on Mobility Management and Wireless Access (MobiWac)*, páginas 61–68, Florida, EUA, noviembre 2011.
- [100] Mohammed S. Al-kahtani y Hussein T. Mouftah. A stable clustering formation infrastructure protocol in mobile ad hoc networks. En *IEEE International Conference on Wireless And Mobile Computing, Networking And Communications (WiMob)*, páginas 406–413 Vol. 3, Montreal, Canadá, agosto 2005.
- [101] Ching-Chuan Chiang, Winston Liu, Hsiao-Kuang Wu, y Mario Gerla. Routing in clustered multihop mobile wireless networks with fading channel. En *IEEE Singapore International Conference on Networks (SICON)*, páginas 197–211, Singapore, Singapore, abril 1997.
- [102] Uichin Lee, Joon-Sang Park, Seung-Hoon Lee, Won W. Ro, Giovanni Pau, y Mario Gerla. Efficient peer-to-peer file sharing using network coding in MANET. *Journal of Communications and Networks*, 10(4):422–429, diciembre 2008.
- [103] Afzal Mawji y Hossam Hassanein. Efficient multipoint P2P file sharing in MANETs. En *Global Telecommunications Conference (GLOBECOM)*, páginas 1–6, Hawaii, EUA, noviembre 2009.