Centro de Investigación y de Estudios Avanzados del Instituto Politécnico Nacional

Unidad Zacatenco

Departamento de Ingeniería Eléctrica

Sección de Comunicaciones

"Evaluación del impacto de ataques de seguridad en redes sobrepuestas *Peer-to-Peer*."

Tesis que presenta:

Diana Rebeca Ramírez Pavón

Para obtener el grado de:

Maestra en Ciencias

Directores de Tesis:

Dr. Domingo Lara Rodríguez

Dr. Raúl García Ruiz

México, Ciudad de México Febrero, 2016

A mi familia:

Antonio y Osiris,

Omar y Melissa,

Rocko y Petit

AGRADECIMIENTOS

A mis papás, porque me han ayudado y cuidado desde siempre. Porque sin ustedes no sería lo que soy. A mi papá por las desmañanadas, a mi mamá por las desveladas. A mi papá por sus consejos y cuestionamientos, a mi mamá por sus atenciones y preocupaciones.

A mis hermanos, por todos los momentos vividos, por aguantarme y acompañarme.

A mis asesores, Dr. Domingo Lara y Dr. Raúl García Ruíz, por haberme brindado la oportunidad de trabajar con ustedes y crecer.

Al Consejo Nacional de Ciencia y Tecnología (CONACYT) por apoyarme económicamente durante la duración de la maestría.

Al Centro de Investigación y de Estudios Avanzados del I.P.N. (CINVESTAV), por brindarme las facilidades para realizar mis estudios de posgrado.

A los investigadores de la sección de Comunicaciones, que con sus clases y asesorías, enriquecieron mi formación.

Al personal de la sección de Comunicaciones, por el apoyo brindado.

A mis compañeros de maestría: Ángel, Gerardo, Felipe, Víctor y Alavid; por todas las mañanas, tardes y noches de trabajo juntos.

A mis amigos, por apoyarme en los momentos de estrés y no dejarme flaquear cuando lo necesité.

A Tona, porque sin tu apoyo y guía no lo habría podido hacer. Por soportarme, por entenderme, por ayudarme a ver de lo que soy capaz y no dudar de mí.

RESUMEN

En años recientes, han emergido varias aplicaciones de escritorio que utilizan un modelo descentralizado para la conexión simultánea de usuarios múltiples. Estas aplicaciones permiten la compartición de archivos, la creación de grupos sociales o simplemente la comunicación entre diferentes usuarios en redes a gran escala. Debido a su arquitectura descentralizada, estas aplicaciones se implementan sobre redes *Peer-to-Peer* (P2P), en donde se elimina el uso de servidores como intermediarios en la comunicación y se utilizan redes sobrepuestas para su estructuración.

Las redes P2P presentan características que las hacen adecuadas y flexibles para muchas aplicaciones como lo son su escalabilidad y un ambiente abierto. Sin embargo, son estas características las que también la hacen vulnerable a peligros de seguridad. Debido a que no se tiene una dependencia de servidores para realizar las funciones de la red, sino que éstas están distribuidas entre todos los usuarios de la red, es posible que usuarios maliciosos alteren los procedimientos funcionales del sistema de manera egoísta o malintencionada.

Hoy en día existen diversos ataques a la seguridad en redes sobrepuestas P2P, enfocados a diferentes operaciones y servicios del sistema. En este trabajo se hace un estudio de los ataques reportados en la literatura en redes sobrepuestas de tipo estructurada. Además, se incluye una revisión de las soluciones o contraataques presentados previamente, evaluando la seguridad que proporcionan, así como otros aspectos que conllevan su implementación. De manera particular, se abordan los ataques relacionados a la presencia de nodos maliciosos y su influencia en los procedimientos de almacenamiento y enrutamiento de una red sobrepuesta de tipo Chord. Para medir el riesgo y daño que genera un porcentaje de nodos realizando un ataque en particular de manera simultánea, se propuso un análisis para evaluar la media del número de saltos en la red, así como la probabilidad de búsqueda exitosa.

Por último, se estudia la seguridad proporcionada por el actual protocolo para señalización de redes P2P de la IETF, RELOAD, principalmente en la implementación de la red sobrepuesta recomendada, cuya estructura está basada en el protocolo Chord. En el estudio del protocolo RELOAD, se propone una solución para minimizar los efectos de los ataques residuales presentes. La solución se evalúa bajo los parámetros de desempeño mencionados, para mostrar las propiedades de seguridad que aporta a una red sobrepuesta Chord-RELOAD.

ABSTRACT

In the last years, there have been an increasing emergence of desktop applications that use a decentralized model to connect users simultaneously. These applications include, among others, file sharing capacities, facilities to support social networks, and the ability to bring communication to users in large scale networks. Due to their decentralized nature, these applications use the concept of Peer-to-Peer networking. P2P eliminates servers as intermediates in the communication and uses overlay networks for the network architecture.

Peer-to-Peer networks feature scalability and openness which provide them the flexibility needed in many modern applications. However, these features also make them vulnerable to security risks. Due to the lack of centralized control and a distributed task methodology, malicious peers have the opportunity to alter or disrupt the functionality of the system, which makes security in P2P networks a topic of great relevance.

There have been several works devoted to security in P2P overlay networks, focused in strengthening different modules and services of the system. In this work, a review has been made about the different attacks reported in the open literature that affect structured overlay networks. Throughout this review, a summary of the counterattacks and security measures for these attacks is also presented, evaluating the features and costs introduced by their implementation. In particular, this work studies the vulnerabilities that the Chord protocol presents under the presence of malicious nodes, which disturb the storage and routing mechanisms. An analysis to evaluate the routing performance is proposed in order to review the impact introduced by the presence of subversive peers in the network.

Finally, a review of the security scheme of the P2P signaling protocol, RELOAD, is addressed; specifically, the topology plug-in module defined in the specification 6940, which is a DHT modification based on Chord. As a result of the analysis made in RELOAD's security, a proposal is given to reduce the effect of the founded residual attacks. The routing performance of the enhanced network is evaluated to measure the effects of the proposed solution.

CONTENIDO

LISTA DE FIGURAS

LISTA DE TABLAS

INTRODUCCIÓN

El modelo *Peer-to-Peer* (P2P) es un modelo computacional distribuido realizado para la compartición y manejo de recursos de manera masiva. Su fundamento principal es que todos los nodos en la red tienen una relación equitativa, donde cada uno actúa de cliente y de servidor dentro del sistema. En la arquitectura tradicional cliente-servidor, el servidor es el que recibe todas las peticiones de los usuarios y maneja los recursos para cumplir con los servicios proporcionados por la red. En este modelo, los servidores suelen ser un obstáculo para la escalabilidad de la red, puesto que actúan como cuello de botella en la realización y prestación de los servicios de un sistema. En el modelo P2P no existen nodos centrales que limiten el desempeño de la red, sino que son los pares los que de manera distribuida manejan los recursos de todo el sistema para brindar uno o varios servicios. Los nodos de una red P2P aportan al sistema parte de sus recursos, como por ejemplo, recursos de almacenamiento o procesamiento, los cuales son compartidos con los demás pares del sistema para llevar a cabo las funciones de la red. Esta auto-organización permite que el crecimiento de la red no afecte el desempeño de las aplicaciones ejecutadas sobre la misma, haciendo del modelo P2P una alternativa preferida para servicios de gran escala. La tecnología P2P ha permitido el desarrollo de nuevas aplicaciones a escala de la Internet, entre estas se incluyen los sistemas de compartición de archivos, los sistemas de almacenamiento distribuido, las aplicaciones de ambiente colaborativo distribuido, etc. Actualmente, uno de los sistemas basados en el concepto P2P más popular, es el de *streaming* de contenido multimedia.

Debido a su naturaleza distribuida, en las redes P2P se utilizan redes sobrepuestas que organizan los nodos en una topología determinada, sobre la cual se utilizan mecanismos de búsqueda que permiten localizar un objeto en particular dentro de la red. Estos mecanismos, refieren una llave o cadena determinada a un conjunto de nodos responsables del objeto asociado a este identificador. De manera general, la búsqueda del objeto se puede realizar de manera no estructurada y estructurada. En las redes P2P del tipo no estructurada, los objetos se localizan por medio de técnicas de inundación. Sin embargo, este esquema presenta conflictos con la característica de escalabilidad, deseable en los sistemas P2P, ya que el uso de las técnicas de

inundación incrementa el costo en procesamiento y el tráfico en la red. Además, no proveen garantías en el tiempo de búsqueda, ni en la disponibilidad de los objetos. Por otro lado, las redes de tipo estructurada implementan una tabla hash distribuida (DHT) sobre la topología de la red. Esta abstracción de la DHT permite que se limiten el balance de la carga de los nodos, la manera en que se dirige una búsqueda dentro de la red, así como el tiempo en el que se realiza. En la literatura existen diversas propuestas de redes sobrepuestas de tipo estructurada para redes P2P, entre estas se encuentran: Chord, CAN, Tapestry, Kademlia y Pastry.

La propiedad de descentralización de las redes P2P le brinda, entre otras ventajas, la capacidad de crear redes de gran escala para aplicaciones de ambientes abiertos. Sin embargo, es esta descentralización la que hace vulnerables a los sistemas par-a-par a ataques de seguridad. Debido a que los nodos de la red son los responsables de realizar las tareas de almacenamiento, enrutamiento y mantenimiento del sistema, la seguridad de la red depende de la integridad de los nodos. Si un sistema descentralizado está formado por nodos subversivos que alteran los mecanismos que rigen el funcionamiento del mismo, la información y los servicios que proporcionan las aplicaciones ejecutadas sobre la red se verán amenazados. Existen muchas formas de realizar ataques en una red estructurada sobrepuesta, desde una negación de servicio, hasta la escucha ilegal de mensajes, etc. Sin embargo, los ataques que presentan una mayor amenaza son aquellos que están enfocados a invalidar el mecanismo de recuperación e inserción de un objeto a partir de un identificador en la topología de la red sobrepuesta. Puesto que la principal operación en una red P2P es la de búsqueda de los nodos responsables de un objeto, resulta importante evaluar los alcances de nodos maliciosos que interrumpan o alteren esta operación. Por todo lo anterior, uno de los alcances de esta tesis es el de llevar a cabo una revisión de los ataques que se realizan en los sistemas Peer-to-Peer, así como de las defensas que se pueden implementar para contrarrestarlos.

Actualmente, el protocolo de señalización para redes P2Pde la IETF, RELOAD, brinda los mecanismos y operaciones para proveer un servicio de almacenamiento y de enrutamiento entre pares que forman una red sobrepuesta. De manera particular, la topología de red estructurada que define el protocolo es una modificación de la topología tipo anillo, Chord. En esta topología, los pares se organizan en un espacio de identificadores unidimensional y unidireccional, que proporciona un mecanismo de búsqueda basado en el principio de hash consistente. Esta

implementación de DHT, permite que las búsquedas así como el estado que almacenan los nodos para el enrutamiento tenga una relación $\mathcal{O}(\log N)$, donde N es el tamaño de la red. Además, RELOAD define un modelo de seguridad basado en certificados con el cual brinda protección a nivel de objetos, mensajes y conexiones. A pesar de las estrategias de seguridad presentes en RELOAD, aún existen ataques residuales[1] que limitan el desempeño de la red sobrepuesta. En esta tesis, se evalúa una propuesta para contrarrestar los ataques que pueden realizar nodos maliciosos en una red P2P que utiliza el protocolo RELOAD como protocolo de señalización de la red sobrepuesta.

La organización de esta tesis es la siguiente:

- En el Capítulo 1, se hace una revisión del paradigma *Peer-to-Peer*, introduciendo las características, ventajas y debilidades que ofrece; así como algunas de las aplicaciones que han emergido a partir de este modelo. Asimismo, se revisa el concepto de red sobrepuesta y se profundiza en dos de sus principales arquitecturas estructuradas: Chord y CAN. Por último, se presenta la modificación de Chord en el protocolo RELOAD.
- El Capítulo 2 es una revisión de la seguridad en las redes P2P estructuradas. En éste se exploran los diversos ataques que se pueden llevar a cabo en las operaciones de un sistema P2P, así como algunas de las soluciones presentadas en la literatura.
- En el Capítulo 3, se realiza la evaluación y comparación del desempeño de Chord y CAN referente a la media del número de saltos en una búsqueda, de manera analítica comprobando los resultados por medio de simulación. Además, se introduce una solución que permite encontrar la media del número de saltos en una búsqueda exitosa de manera analítica cuando existen nodos maliciosos en una red de tipo Chord y Chord-RELOAD, así como la probabilidad de búsqueda exitosa. Los resultados de la metodología propuesta se validan por medio de simulación.
- En el Capítulo 4 se plantean ataques residuales que pueden realizarse en una red P2P, con RELOAD como protocolo de señalización de la red sobrepuesta. Por último, se

[1] El término residual se refiere a aquellos ataques que se pueden realizar en el sistema, después de la implementación de las medidas de seguridad.

propone una solución para mitigar los efectos de la presencia de nodos maliciosos en los mecanismos de inserción y recuperación de un objeto en RELOAD.

- Al final del trabajo se presentan las conclusiones resultantes de esta tesis y el posible trabajo a futuro.

CAPÍTULO 1

1. REDES SOBREPUESTAS *PEER-TO-PEER*

En este capítulo se introducen las nociones básicas del paradigma *Peer-to-Peer* (P2P), sus motivaciones y limitaciones, así como las aplicaciones que han popularizado su uso y estudio. Además, se introduce el concepto de una red sobrepuesta y se ilustran dos formas de organización de las redes sobrepuestas comúnmente utilizadas, Chord y CAN. Por último, se presenta el protocolo RELOAD, con el cual desde el punto de vista de la topología de red sobrepuesta se fijan las bases del trabajo desarrollado.

1.1 REDES PEER-TO-PEER

1.1.1 Introducción

Las redes *Peer-to-Peer* han emergido como una arquitectura para aplicaciones que permiten la interacción de miles de usuarios alrededor del mundo sin la dependencia de servidores dedicados, en su representación más formal. Estas redes permiten proporcionar servicios de comunicación, de compartición de archivos, entre otros, por medio de la integración y organización de los recursos de cada uno de los usuarios dentro de la red.

En el 2001 con la masificación de aplicaciones como Gnutella [1], Napster [2] y BitTorrent [3], la popularidad de las redes *P2P* (*Peer-to-Peer*) se extendió a ámbitos tanto académicos como comerciales, impulsados en gran parte por la controversia que presentaba el debate entre las

compañías productoras de material protegido y los creadores de las aplicaciones que permitían su intercambio ilegal [1]. Con la subsecuente disponibilidad de aplicaciones *P2PTV* (*Peer-to-Peer Television*) y *VoP2P* (*Voice over Peer-to-Peer*) se abrió el paso para nuevas líneas de investigación, actualmente populares, como por ejemplo las referentes al *streaming* en tiempo real sobre redes P2P [4], [5]. Como una consecuencia de lo anterior, actualmente el concepto y la tecnología P2P han madurado, permitiendo una extensión en sus capacidades para ofrecer servicios en diferentes áreas con mayor escalabilidad, integridad y variabilidad.

En la actualidad los sistemas P2P, debido a sus características intrínsecas de repartición de responsabilidades y distribución de la información entre todos los usuarios dentro de la red P2P, cuentan con brechas de seguridad en su fundamento que han sido estudiadas e implementadas en los sistemas P2P actuales [6], [7]. Sin embargo, aún existen problemas abiertos referentes a la seguridad que proporcionan los sistemas distribuidos par a par, particularmente aquellos enfocados a redes cuyo objetivo es disminuir la latencia en el enrutamiento en las redes subyacentes. Debido a que en estos sistemas los pares se agrupan de acuerdo a la proximidad física, existen ataques enfocados a perjudicar grupos de nodos en particular [8].

1.1.2 Conceptos P2P

El concepto *Peer-to-Peer*, se utiliza para describir una gran variedad de sistemas con diversas arquitecturas, incluyendo aquellas en las cuales la comunicación no se lleva a cabo entre pares iguales sino que existe una desigualdad entre participantes asemejándose a una arquitectura cliente-servidor. Sin embargo, la definición presentada incluye aspectos propios de una red P2P como lo son la compartición de recursos, auto-organización, descentralización e interconexión:

> Los sistemas *Peer-to-Peer* son sistemas distribuidos que consisten de nodos interconectados entre sí, con la capacidad de auto-organizarse a una topología determinada con el propósito de compartir recursos tales como contenido, ciclos de CPU o almacenamiento. Estos son capaces de adaptarse a fallas y de organizar nodos transitorios, manteniendo una conectividad y un rendimiento aceptables sin requerir de la intermediación de una entidad centralizada [9]

Las siguientes son características que se pueden encontrar en la mayoría de los sistemas P2P [2]:

- Compartición de recursos. Cada par contribuye en la operación del sistema P2P con recursos propios. Idealmente el recurso prestado es proporcional al uso del usuario de los recursos del sistema, sin embargo, cuando se accede al sistema se establece una cuota inferior. La contribución de recursos debería ser mutuamente beneficiosa, por lo que a los usuarios se les motiva a participar haciendo comparable el beneficio contra los recursos prestados.
- Interconexión. Todos los nodos están conectados a otros nodos dentro del sistema P2P, y todo el conjunto de nodos forman un grafo conectado. Cuando dentro del grafo existen nodos que no se encuentran conectados se tiene lo que se conoce como una partición en la red.
- Descentralización. El comportamiento del sistema P2P está determinado por la acción colectiva de los pares sin la existencia de un punto central de control. Sin embargo, algunos sistemas realizan alguna acción por medio de un servidor central, por ejemplo, para asegurar el acceso a la red.
- Simetría. Los nodos tienen roles iguales dentro de la operación del sistema. En el modelo P2P cada par actúa como cliente y también como servidor, solicitando recursos a la red así como dirigiendo búsquedas y almacenando objetos de otros pares en la red. En la práctica éste es un comportamiento idealizado, ya que el tiempo de vida de los pares, la heterogeneidad de los recursos de los nodos en la red o la naturaleza de las redes actuales con el uso de dispositivos traductores de direcciones (*NAT por Network Address Translation*) y *firewalls*, impide que se tenga una correspondencia equitativa en la funcionalidad de los pares. Además, en algunos diseños se relaja esta condición al hacer una división de los nodos en jerarquías.
- Autonomía. La participación del par en el sistema es local, es decir, cada par determina sus capacidades de acuerdo a sus recursos, cada par determina cuando se une al sistema, cuando realiza peticiones y cuando deja el sistema. Esta autonomía puede hacer que los servicios ofrecidos en el sistema se vuelvan impredecibles cuando existe mucha movilidad de los nodos o los nodos deliberadamente limitan su contribución al sistema desconectándose cuando no lo requieren.

- Auto-organización. La organización del sistema P2P es variable en el tiempo de acuerdo al conocimiento y las operaciones locales de los pares.
- Escalabilidad. Ésta es un requisito para los sistemas P2P que operan con una gran cantidad de nodos simultáneamente y se traduce en que los recursos que utiliza cada par presentan una variación con respecto al tamaño de la red, sucediendo lo mismo con el tiempo de respuesta.
- Estabilidad. Bajo condiciones de dinamismo en la red (*churn*), entrada y salida de usuarios en la red, el grafo de la misma debe ser capaz de dirigir una búsqueda de manera exitosa. Ya que los pares no cuentan con una visión general del estado de la red, para el envío de mensajes dentro de la red se requiere de nodos intermedios que dirijan la búsqueda a la región correcta en la red, por lo que cuando los nodos entran y salen de esta las trayectorias de enrutamiento se ven afectados.

Un sistema P2P básico se puede dividir en tres módulos [10]:

- Módulo de enrutamiento y re-envío de mensajes.
- Módulo de búsqueda y almacenamiento de contenido.
- Módulo de configuración y selección de los pares.

Módulo de enrutamiento y re-envío de mensajes.

Bajo este módulo se llevan a cabo procedimientos para que cada par mantenga un estado de conexión con sus pares vecinos dentro de la red. El mantenimiento de este estado puede incluir el descubrimiento de nuevos vecinos y la verificación de los vecinos actuales. Así mismo, el módulo especifica un mecanismo para la localización de pares mediante los cuales se lleva a cabo la admisión a la red (*bootstrap*), así como protocolos para realizar la unión y salida de pares de la red.

Las funciones de re-envío de mensajes a través de nodos intermediarios también están especificadas dentro de este módulo, así como la interacción entre pares hacia y por medio de la aplicación del sistema P2P.

Módulo de búsqueda y almacenamiento de contenido.

En el caso de una aplicación básica, cómo un sistema de compartición de archivos, este módulo es el encargado de distribuir el contenido entre los pares disponibles en la red, además de proveer métodos de búsqueda y en caso de requerirse para la aplicación, proporcionar métodos para el almacenamiento de objetos con prioridad o con baja demanda.

Módulo de configuración y selección de los pares.

Éste determina la utilización de los recursos del par, así como su rol dentro de la red. El par determina los recursos disponibles al inicio de una sesión dentro del sistema y puede monitorearlos periódicamente o realizar cambios en caso de que el uso de la aplicación lo requiera. El rol del par en el sistema está basado en sus capacidades, por ejemplo, si se trata de una arquitectura jerárquica un súper nodo debe proporcionar cierta estabilidad, puesto que un gran número de peticiones se realizará a través de él.

1.1.3 Motivación y potencial de las redes P2P

Muchos servicios proporcionados por Internet se distribuyen utilizando el modelo cliente-servidor, en esta arquitectura los clientes se conectan a un servidor utilizando algún protocolo de comunicación para obtener algún recurso en específico. La mayor parte del procesamiento realizado para proveer el servicio se lleva a cabo del lado del servidor, por lo que cuando existe un aumento en el número de clientes, el servidor puede sufrir congestionamiento y eventualmente, si el número de peticiones continúa incrementando, el servidor se vuelve incapaz de responderlas o inclusive puede fallar. La principal ventaja de este modelo es que del lado del cliente se requiere un menor número de recursos, pero también requiere que el servidor aumente sus capacidades para brindar un mejor servicio a una mayor cantidad de clientes.

Por otra parte, en una arquitectura P2P se tiene la habilidad de brindar servicios con una mayor disponibilidad a un menor costo, al maximizar el uso de los recursos de cada nodo conectado en

la red. Mientras que el modelo cliente-servidor se sustenta en las capacidades del servidor para proveer un servicio robusto, en P2P se puede ofrecer el mismo nivel de robustez si las demandas del servicio se dispersan entre toda la red.

Adicionalmente, cuando se tiene una mayor descentralización del sistema se tiene una mejoría en la tolerancia a fallas del servicio brindado, ya que éste se reparte entre todos los pares de la red.

La popularidad de los esquemas P2P se sustenta en los beneficios que ésta proporciona a los clientes en comparación con una arquitectura cliente-servidor, por ejemplo:

- P2P le permite a los usuarios liberarse de la dependencia de los servidores, brindándoles la facilidad de compartir contenido (por ejemplo música, videos, videojuegos, software, etc.) sin la necesidad de descargarlos o subirlos al servidor.
- P2P disminuye la vulnerabilidad a puntos de falla únicos muy comunes en el modelo cliente-servidor.
- P2P brinda una interacción usuario-usuario lo que elimina los retardos generados por el servidor al responder a peticiones.
- Muchas aplicaciones P2P ofrecen el uso de canales virtuales de comunicación capaces de disminuir los obstáculos impuestos por el uso de redes privadas como lo son los *firewalls* y NAT.
- P2P proporciona una mayor disponibilidad del contenido y del servicio suministrado, esto debido a que un nodo puede ser redirigido por múltiples nodos en caso de falla de algún nodo intermediario, así como puede obtener el recurso de un conjunto de nodos.
- P2P es inherentemente auto-escalable ya que con cada nuevo usuario que ingresa a la red se incrementa la capacidad del sistema en sí.

1.1.4 Retos en P2P

Los sistemas P2P proporcionan una gran variedad de características que los hace adecuados para ofrecer servicios de aplicaciones orientadas a un gran número de usuarios interactuando simultáneamente, sin embargo estas características también imponen limitaciones y retos en el diseño del sistema.

La auto-escalabilidad de una red P2P permite incrementar la capacidad de la misma con cada nuevo usuario, no obstante no todos los usuarios cuentan con los mismos recursos para ofrecer o pueden introducir dificultades en el enrutamiento de mensajes dentro de la red, por ejemplo si están detrás de un *firewall*. Es por esta razón que la auto-escalabilidad no puede traducirse directamente a un incremento en el rendimiento de la red, ya que la carga en el sistema puede no encontrarse uniformemente distribuida. Por ejemplo, cuando se tiene algún objeto que se vuelve muy popular, gran parte de las peticiones se centrarían en aquellos nodos que cuentan con el objeto deseado o que se encuentran en la ruta para el mismo.

Dado que el tiempo de vida de un usuario P2P es impredecible, el diseño de un sistema P2P debe compensar la variabilidad presentada ante el dinamismo de los usuarios en la red, además se debe asegurar la confiabilidad del servicio. En general, la confiabilidad se traduce en redundancia, por ejemplo se pueden colocar copias de los objetos en varios nodos y así incrementar la disponibilidad del objeto, o podría incrementarse el conjunto de nodos utilizados para dirigir las peticiones y de esta manera aumentar la probabilidad de un ruteo exitoso. Sin embargo, el uso de redundancia se ve reflejado en un incremento en la información intercambiada entre los pares para el mantenimiento de la red.

En el caso de los sistemas P2P se idealiza el comportamiento de los usuarios: cada par en la red proporciona recursos altruistamente, no tienen un comportamiento malicioso, etc. No obstante, en la realidad los usuarios actúan de acuerdo a sus propios intereses interfiriendo con la operación ideal del sistema. Sin la presencia de un control centralizado resulta difícil validar las intenciones de los usuarios y monitorear sus acciones, pero este control resulta contrario al modelo descentralizado de P2P, por lo que en el diseño de un sistema P2P es necesario un compromiso entre la escalabilidad que proporciona una naturaleza distribuida y la seguridad proporcionada por entidades centralizadas.

1.1.5 Aplicaciones P2P

Entre las aplicaciones P2P se encuentran la compartición de archivos, mensajería instantánea, VoP2P, *streaming*, computo de alto rendimiento, motores de búsqueda, etc.

Sistemas para la compartición de archivos

Los sistemas para la compartición de archivos pueden dividirse en 3 categorías de acuerdo con el grado de centralización que tienen:

1. Redes P2P centralizadas. A pesar de que el paradigma P2P se considera un opuesto al cliente-servidor, la primera generación de este tipo de sistemas, por ejemplo, Napster o BitTorrent, contaba con un servidor que almacenaba la meta-información de los objetos compartidos, como podría ser la dirección o identificadores de los nodos que contaban con el objeto deseado, pero el intercambio del contenido se realizaba entre pares.
2. Redes P2P descentralizadas. Para resolver los problemas que presentaban las redes P2P centralizadas, como lo son la escalabilidad y la tolerancia a fallas, se desarrollaron redes descentralizadas que no dependían de un servidor central, entre las cuales las más populares fueron Gnutella y Freenet [11]. Para realizar las operaciones de envío de mensajes, búsqueda y almacenamiento de contenido se hace por medio de inundación desde un nodo hacia sus nodos vecinos los cuales así mismo re-envían las peticiones a sus vecinos y sucesivamente así hasta localizar al nodo destino.
3. Redes P2P híbridas. Dados los problemas que presenta la inundación de peticiones en las redes P2P descentralizadas se desarrolló una nueva generación de redes híbridas con una arquitectura jerárquica. Entre los sistemas populares se encuentran KaZaA [2] o JXTA [12].

Sistemas de Voz sobre P2P

Los sistemas de telefonía P2P proporcionan los servicios que permite la Voz sobre IP (VoIP) pero con los beneficios que brinda una arquitectura P2P, como lo son: incremento en la disponibilidad del servicio, escalabilidad y poca dependencia de una infraestructura dedicada.

Los fundadores de KaZaA, posteriormente, desarrollaron la primera aplicación ampliamente utilizada de voz sobre P2P: Skype [13]. Actualmente Skype cuenta con más de 300 millones de usuarios registrados y hasta 43 millones de usuarios activos diariamente [14], provee servicios de

llamadas de voz y de video, así como de mensajería instantánea, intercambio de archivos y videoconferencias, entre otros. El diseño de Skype se cree está basado en un esquema P2P jerárquico de acuerdo con estudios realizados previamente [15] [16].

Sistemas de *streaming* de contenido

En este tipo de sistemas, uno o varios pares que poseen todo o una parte del contenido lo envían a los pares solicitantes, y estos mismos pueden convertirse posteriormente en proveedores del contenido que se consume mientras sigue siendo transferido. Los servicios más comunes son aquellos de video bajo demanda o de transmisión de televisión en vivo. Algunas aplicaciones actuales que ofrecen este tipo de servicios son SopCast [17] y PPS.tv [18].

1.2 REDES SOBREPUESTAS P2P

1.2.1 Introducción

Los pares en las aplicaciones P2P se comunican con otros pares utilizando mensajes que se transmiten sobre la Internet o alguna otra red. El protocolo de una aplicación P2P, que establece este intercambio de mensajes y las acciones al recibirlos o enviarlos, se construye sobre la capa de aplicación de la pila de protocolos de la red sobre la que está el servicio de la misma, de esta forma se abstrae la conectividad de los nodos miembros de la red subyacente e se independiza de la implementación P2P, mediante el uso de redes sobrepuestas (*overlay networks*) o redes sobrepuestas P2P (*P2P overlay*). Ver Figura 1.1.

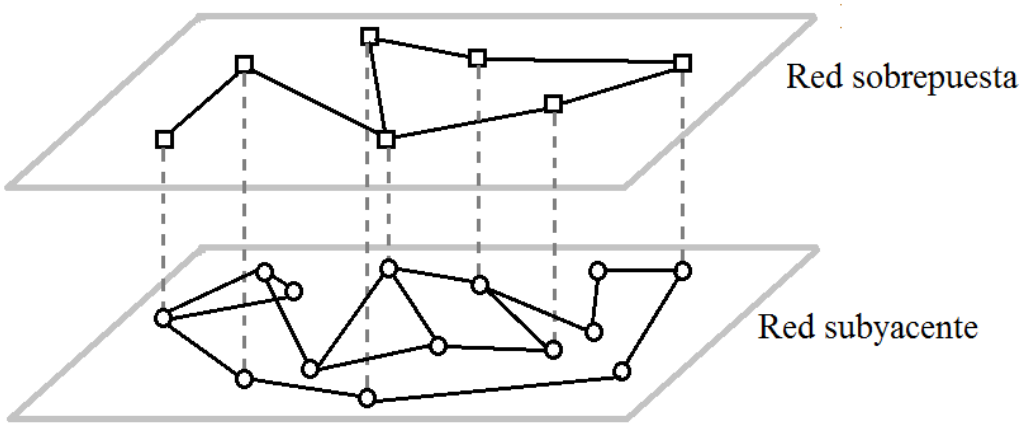


Figura 1.1. Construcción de una red sobrepuesta sobre la red subyacente.

Una definición de una red sobrepuesta es:

> Una red sobrepuesta es una capa de aplicación virtual o lógica en la cual los dispositivos terminales pueden ser direccionados y que brinda conectividad, enrutamiento y envío de mensajes entre los mismos. Las redes sobrepuestas son usadas frecuentemente como un sustrato para desarrollar nuevos servicios de red, o para crear una topología de enrutamiento que no está presente en la red subyacente física [10].

1.2.2 Clasificación de las redes sobrepuestas P2P

Los diseños de los diferentes sistemas P2P existentes y las redes sobrepuestas utilizadas en los mismos se pueden clasificar en:

- Redes sobrepuestas estructuradas y no estructuradas.
- Redes sobrepuestas jerárquicas.
- Redes sobrepuestas de servicio.

Redes sobrepuestas no estructuradas.

Una red sobrepuesta no estructurada es aquella en la cual un nodo sólo depende de sus nodos adyacentes para el envío de mensajes a otros nodos dentro de la red, algunos ejemplos de estrategias de propagación de los mensajes son por medio de inundación o por caminatas aleatorias [10]. Algunos ejemplos de redes sobrepuestas no estructuradas son Gnutella y Freenet.

Redes sobrepuestas estructuradas.

Una red sobrepuesta estructurada es aquella en la cual los nodos mantienen información que les permite llegar a todos los nodos en la red [10]. A comparación de las redes sobrepuestas no estructuradas, éstas proporcionan un límite en el número de mensajes que se requieren para encontrar un recurso en la red. Para poder llevar a cabo este ruteo determinístico, los pares se ubican en un espacio de direcciones virtual, la red sobrepuesta se organiza en base a una geometría determinada y se utiliza una función para mapear un recurso a un nodo dentro del espacio virtual. La mayoría de las redes sobrepuestas estructuradas utiliza un procedimiento de ruteo basado en identificadores, en este caso un conjunto de identificadores se asocia con una dirección dentro del espacio de direcciones de tal forma que el nodo cercano a esa dirección será el responsable de almacenar los recursos asociados a esos identificadores. Una tabla hash distribuida (*Distributed Hash Table, DHT*) se utiliza en las redes sobrepuestas estructuradas como un mecanismo distribuido de indexación para resolver peticiones de búsqueda [19]. Algunos ejemplos de protocolos de redes sobrepuestas basadas en DHT son Chord [20], CAN [21], Kademlia [22], Pastry [23] y Tapestry [24]. En las siguientes secciones se analizan Chord y CAN con mayor profundidad.

Redes sobrepuestas jerárquicas.

Una red sobrepuesta jerárquica es aquella en la cual se tienen múltiples redes sobrepuestas anidadas e interconectadas en un árbol. Los mensajes entre diferentes redes sobrepuestas se

encaminan hacia el nodo más cercano en la jerarquía, con la opción de tener diversos procedimientos de enrutamiento en cada red sobrepuesta. Este tipo de redes pueden utilizarse para mejorar la eficiencia del sistema cuando se tienen distribuciones concentradas por regiones.

Redes sobrepuestas de servicio.

Para acelerar el desarrollo de nuevos servicios y evitar cambios en la infraestructura de la red existente, muchos servicios se han implementado como protocolos de la capa de aplicaciones, como por ejemplo la Voz sobre IP o las redes de entrega de contenidos (*Content Delivery Networks, CDN*), cuando una red sobrepuesta se utiliza como base para este tipo de aplicaciones se le refiere como una red sobrepuesta de servicio.

1.3 CHORD

1.3.1 Introducción

El protocolo Chord [20] es un protocolo escalable de búsqueda dentro de un sistema P2P que cuenta con entradas y salidas dinámicas. Su operación primordial es dada una llave la mapea a un nodo, dependiendo de la aplicación encima de la red sobrepuesta Chord, el nodo puede almacenar algún valor asociado a esta llave. Para realizar la asignación llave-nodo en el protocolo Chord se utiliza *consistent hashing* [25], ya que éste tiende a balancear la carga entre los nodos de la red y limita las alteraciones que sufren las llaves en la entrada y salida de nodos de manera local. Sin embargo, Chord mejora la escalabilidad presente en *consistent hashing* donde todos los nodos deben estar conscientes de los demás nodos en la red.

En Chord los pares se organizan sobre la red sobrepuesta en un anillo lógico. Los pares, para poder realizar una búsqueda, mantienen apuntadores a sus vecinos situados en intervalos logarítmicos sobre el anillo así como enlaces a su predecesor y a su sucesor en el anillo.

Chord presenta las siguientes características:

- Balance de carga. Chord actúa como una función hash distribuida distribuyendo las llaves uniformemente entre todos los pares de la red.
- Descentralización. Chord es totalmente distribuido, es decir no existen nodos con menor o mayor ventaja o prioridad dentro de las funciones de la red.
- Escalabilidad. El costo de una búsqueda en Chord aumenta logarítmicamente conforme al número de pares en la red, lo que permite que redes de gran escala sean realizables.
- Disponibilidad. Las tablas de enrutamiento en Chord se ajustan a las entradas, salidas o fallas de nodos en la red de tal manera que cualquier nodo responsable de una llave puede ser localizado.

La aplicación sobre la que se construye Chord interactúa con este proveyéndole una función que permite la obtención de la dirección IP del nodo responsable de una llave en particular y por medio de notificaciones de los cambios en el conjunto de llaves de las cuales un par es responsable.

1.3.2 Construcción del anillo Chord

La función hash consistente asigna a cada nodo o llave un identificador de m bits utilizando SHA-1 como función base. El identificador de un nodo se obtiene al aplicar la función hash a la dirección IP del nodo, así mismo el identificador de un objeto o llave se obtiene a aplicarle la función hash a la llave. Para evitar que al aplicar la función hash a dos identificadores diferentes se obtenga el mismo resultado se escoge m suficientemente grande, de tal forma que la probabilidad de que este evento ocurra sea despreciable.

La asignación de llaves a nodos en *consistent hashing* se hace de la siguiente manera: los identificadores se ordenan en un círculo modulo 2^m, la llave k se asigna al nodo inmediato cuyo identificador sea igual o mayor al identificador k en el espacio de identificadores, ver Figura 1.2. A este nodo se le conoce como el sucesor de la llave k, en la representación del espacio de identificadores como un círculo con números del 0 a 2^m, el sucesor de k sería aquel que se encuentra inmediatamente después en sentido de las manecillas del reloj.

En *consistent hashing,* si la función hash tiene una distribución uniforme, con alta probabilidad K llaves serán distribuidas en N número de nodos de tal forma que cada nodo es responsable de $(1+\epsilon)\,K/N$ llaves, por lo que se espera una distribución de la carga uniforme en el anillo.

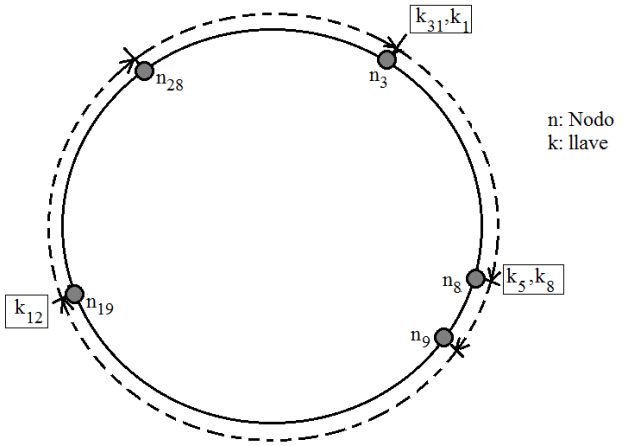


Figura 1.2. Espacio de identificadores en Chord, con $m = 5$.

1.3.3 Búsqueda dentro de la red sobrepuesta

En el protocolo Chord se especifican dos formas de realizar la búsqueda de una llave dentro del anillo Chord:

- Método de localización simple.
- Método de localización escalable.

Método de localización simple

La búsqueda se puede llevar a cabo con el mínimo de almacenamiento de información para el enrutamiento, ya que cada nodo puede mantener el enlace únicamente con su sucesor, entonces las búsquedas se realizarían salto a salto alrededor del círculo pasando sucesor por sucesor hasta encontrar aquel responsable de la llave deseada, como se muestra en la Figura 1.3. Por último, el resultado regresa por la misma trayectoria que siguió la búsqueda.

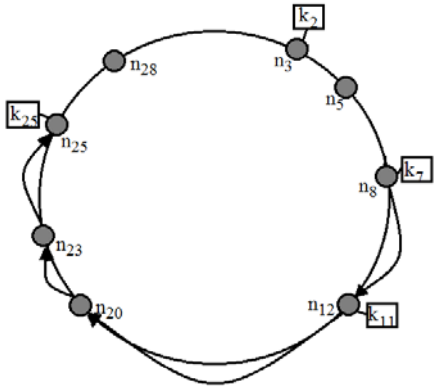
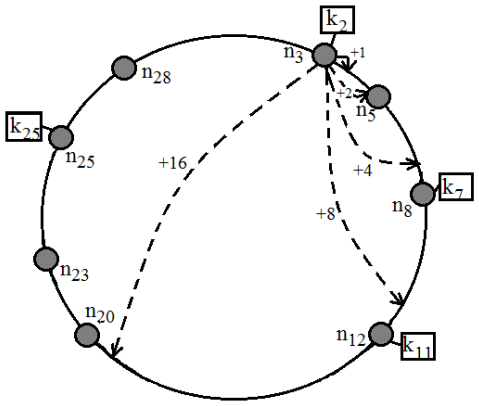


Figura 1.3. Obtención de la llave 25 desde el nodo 8.

Método de localización escalable

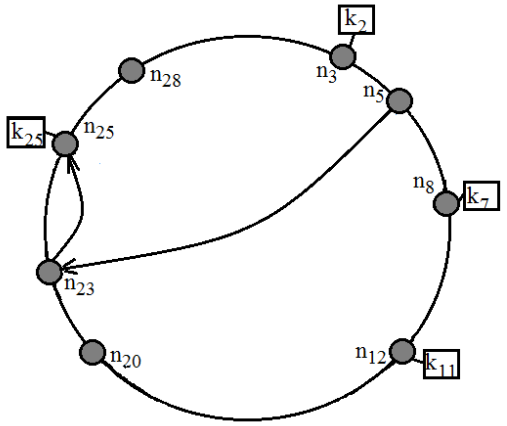
El método anterior requiere de un número idéntico de mensajes a los nodos por los que pasa la búsqueda. Para poder mejorar las búsquedas, en Chord se incrementa la información de enrutamiento de la siguiente forma: Si m es el número de bits de los identificadores del sistema, entonces cada nodo almacena m entradas en su tabla de enrutamiento, llamada tabla de dedos (*finger table*). La entrada i-ésima en la tabla del nodo n corresponde al nodo inmediato s que sucede a n por al menos 2^{i-1} en el espacio de identificadores es decir $s = sucesor(n + 2^{i-1})$ donde $1 \leq i \leq m$ y la aritmética es en modulo 2^m. El nodo s se refiere como el dedo i-ésimo del nodo n. En la Figura 1.4 se muestra un ejemplo de la tabla de dedos del nodo 3.



i	$(n + 2^{i-1})$	Dedo
1	$n_3 + 1$	n_5
2	$n_3 + 2$	n_5
3	$n_3 + 4$	n_8
4	$n_3 + 8$	n_{12}
5	$n_3 + 16$	n_{20}

Figura 1.4. Tabla de dedos del nodo 3.

Para realizar una búsqueda de una llave k desde un nodo n, primero se verifica que k no esté en el intervalo entre n y su sucesor de ser así se regresa el identificador del sucesor y se da por terminada la búsqueda. De lo contrario, se busca en la tabla de dedos de n a aquel dedo cuyo identificador preceda inmediatamente a k y se dirige la búsqueda hacia este dedo, el cual procede de semejante manera, como se muestra en Figura 1.5.



i	$(n + 2^{i-1})$	Dedo
1	$n_5 + 1$	n_8
2	$n_5 + 2$	n_8
3	$n_5 + 4$	n_{12}
4	$n_5 + 8$	n_{20}
5	$n_5 + 16$	n_{23}

Figura 1.5. Búsqueda de la llave 25 realizada por el nodo 5. Se muestra la tabla de dedos del nodo 5.

Este esquema tiene las siguientes características importantes:

- Los nodos sólo almacenan una cantidad de información reducida de otros nodos en la red.
- Los nodos tienen mayor conocimiento de los nodos que están más cercanos a ellos en el espacio de identificadores.
- La tabla de dedos de un nodo no posee toda la información necesaria para determinar el sucesor de cada uno de los nodos en la red.
- Ya que cada nodo tiene entradas apuntando a potencias de dos dentro del espacio de identificadores, la distancia entre el nodo y la llave deseada se va disminuyendo por lo menos a la mitad a cada salto que se realiza, por lo que con alta probabilidad el número de mensajes necesarios para realizar una búsqueda será $O(\log N)$ donde N es el número de nodos en la red.

- En general, el número de nodos a ser contactados en una búsqueda se pueden determinar como el número de unos en la representación de la distancia desde el nodo origen al destino. Dado que se asume que se tiene una distribución uniforme de los nodos dentro del espacio de identificadores se espera que la mitad de los bits en la cadena sean uno. Adicionalmente, cómo se especificó anteriormente, se supone una reducción en la mitad de la distancia a cada salto, por lo que en promedio la longitud de una búsqueda será de $^1/_2 \log_2 N$ saltos.

1.3.4 Mantenimiento de la red sobrepuesta

Para soportar la entrada y salida de usuarios en la red sobrepuesta Chord implementa mecanismos para la unión y partida de nodos preservando la disponibilidad de las llaves almacenadas dentro del anillo.

Unión de nodos en la red

Cuando un nuevo nodo n entra en el sistema, con la ayuda de un nodo en la red localiza a su sucesor dentro del espacio de identificadores y lo ajusta a su tabla de enrutamiento. Periódicamente los nodos ejecutan el mecanismo de estabilización con el que se identifican a los nuevos nodos y se ajustan las tablas de enrutamiento afectadas. El mecanismo consiste en verificar que el sucesor actual del nodo ejecutante sea realmente el sucesor existente en la tabla de ruteo, en el caso de que estos dos no coincidan se modifica la tabla para introducir al nuevo sucesor, lo mismo ocurre para los nodos dedos y el predecesor.

Salida o falla de nodos en la red

En el protocolo Chord el mecanismo de salida de un nodo se maneja de igual forma, ya sea si esta salida es voluntaria o debido a fallas. La validez de las búsquedas en Chord está basada en el hecho de que cada nodo conoce con exactitud a su sucesor. Si el sucesor es incorrecto, la

búsqueda puede resultar fallida. En Chord, adicionalmente a su tabla de dedos, se incluyen una lista de los primeros r sucesores del nodo, para incrementar la robustez ante fallas y asegurar búsquedas correctas. Si el sucesor inmediato del nodo no responde a la petición, el nodo puede sustituir su entrada en la tabla con su sucesor y eventualmente con el mecanismo de estabilización eliminar por completo al nodo fallido o si se trata de una salida voluntaria el nodo saliente puede ejecutar el mecanismo de estabilización para notificar de su partida de manera proactiva.

La lista de sucesores brinda además soporte para replicación a nivel de la aplicación, puesto que en cada nodo dentro del conjunto de sucesores se pueden almacenar copias de los objetos para mejorar la disponibilidad de los mismos.

1.4 CAN

1.4.1 Introducción

CAN (*Content Addressable Network*) [21] es una tabla hash distribuida estructurada de múltiples saltos d-dimensional. Las operaciones básicas de CAN son la inserción, búsqueda y eliminación de pares $(llave\ ,valor)$. La red CAN está constituida de múltiples nodos individuales cada uno de ellos almacena un pedazo (*chunk*) o zona de toda la tabla distribuida, además de mantener información de zonas adyacentes. Las solicitudes para una llave determinada se enrutan por medio de los nodos intermedios adyacentes a la zona deseada. El diseño de CAN permite que sea escalable, totalmente distribuido y tolerante a fallas.

1.4.2 Construcción de CAN

El espacio de identificadores de CAN es un espacio coordenado sobre un toroide d-dimensional. El espacio coordenado se reparte dinámicamente entre todos los nodos del sistema, de tal forma que cada uno de los pares posee una porción limitada del espacio.

El almacenamiento de un par $(llave\ , valor) = (K, V)$ en el espacio d-dimensional se realiza de la siguiente forma:

i. La llave K se mapea a un punto P dentro del espacio coordenado mediante el uso de una función hash uniforme.
ii. El nodo que es responsable de la zona donde el punto P se encuentra almacena el par (K, V).

Para obtener el valor correspondiente a K se procede inversamente, obteniendo el punto P al que está mapeada la llave para obtener la zona a la cual se debe redirigir la búsqueda. En caso de que el nodo solicitante o alguno de sus vecinos sea responsable del valor la solicitud se debe enrutar a través del espacio coordinado hasta la zona resultante.

1.4.3 Búsqueda dentro de la red sobrepuesta

El enrutamiento sobre CAN se hace de tal forma que se siga una línea recta a través del espacio coordenado desde el nodo solicitante u origen hasta el nodo responsable de la zona destino. Para poder dirigir las búsquedas sobre la red cada nodo mantiene un listado de sus nodos vecinos o adyacentes en el espacio coordenado, almacenando la dirección IP y la región de la cual son responsables. En este espacio d-dimensional, dos nodos son vecinos si sus regiones se traslapan en $d - 1$ dimensiones y están en contacto en una dimensión, como se muestra en la Figura 1.6.

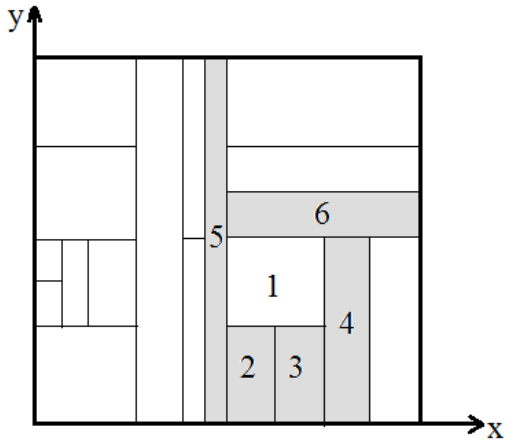


Figura 1.6. Conjunto de vecinos del nodo 1, en un espacio coordenado de 2 dimensiones.

Al realizar la construcción de la red sobrepuesta con el espacio se fraccionado en n zonas de igual tamaño, la trayectoria promedio es de $\left(d/4\right)\left(n^{1/d}\right)$ saltos y cada nodo cuenta con $2d$ vecinos, proporcionando escalabilidad a la red.

Debido a que no existe una sola ruta entre dos puntos en el espacio, aún con fallas en los vecinos se puede lograr una búsqueda exitosa.

1.4.4 Mantenimiento de la red sobrepuesta

Dado que el espacio coordenado se divide entre todos los nodos en la red, el espacio debe reconfigurarse cuando ingresa o sale un nodo.

Unión de nodos en la red

Cuando un nuevo nodo ingresa en la red se le asigna una porción del espacio de la cual se hace responsable, esto se realiza por medio de dividir la zona por la mitad de un nodo existente y repartir los valores pertenecientes a la zona asignada. Por último se notifica a los vecinos de la zona dividida para que se actualicen sus tablas de enrutamiento y así asegurar búsquedas exitosas. La adición de nuevos nodos en la red entonces sólo afecta regiones de manera local, particularmente $O \log d$ nodos.

Salida o falla de nodos en la red

La congruencia del espacio coordenado cuando un nodo sale de la red, se mantiene asegurando que las zonas sean recuperadas por nodos activos. En concreto son los nodos vecinos del nodo saliente los que retoman la zona del mismo, integrándola a su zona actual; del conjunto de nodos vecinos se escoge a aquel que se encuentre activo y que tenga la zona de menor tamaño, para mantener el balance de carga en la red.

1.5 RELOAD

1.5.1 Introducción

REsource LOcation And Discovery (RELOAD) [26] es un protocolo de señalización P2P, producto del grupo de trabajo de la IETF previamente enfocado al desarrollo de protocolos para P2PSIP. El objetivo del grupo de protocolos *Peer-to-Peer SIP* es utilizar una tabla hash distribuida para realizar las operaciones de los agentes SIP encargados del registro de usuarios en la red y para el contacto entre participantes de una sesión y así eliminar la dependencia de servidores y proxys para construir un sistema de inicio de sesiones multimedia distribuido.

Estas operaciones en P2PSIP se realizan de la siguiente forma:

- Registro: Los agentes de usuario utilizan la red sobrepuesta para almacenar y obtener direcciones de contacto mapeadas a identificadores en esta.
- Contacto: Para iniciar una sesión multimedia, una vez que el usuario ha identificado a quien desea llamar, lo localiza por medio de la red sobrepuesta obteniendo su dirección de contacto actual y así posteriormente establecer una conexión directa con este.

Cabe resaltar que P2PSIP sólo se utiliza para almacenar direcciones de contacto o para obtenerlas, una vez que se adquieren se hace la conexión directa entre los pares involucrados y el inicio de la sesión se hace de acuerdo a lo establecido por SIP. Así mismo la información multimedia, una vez establecida la sesión SIP, nunca atraviesa la red sobrepuesta. En la siguiente figura se muestra una comparativa entre el comportamiento para la realización de una llamada en SIP y en P2PSIP.

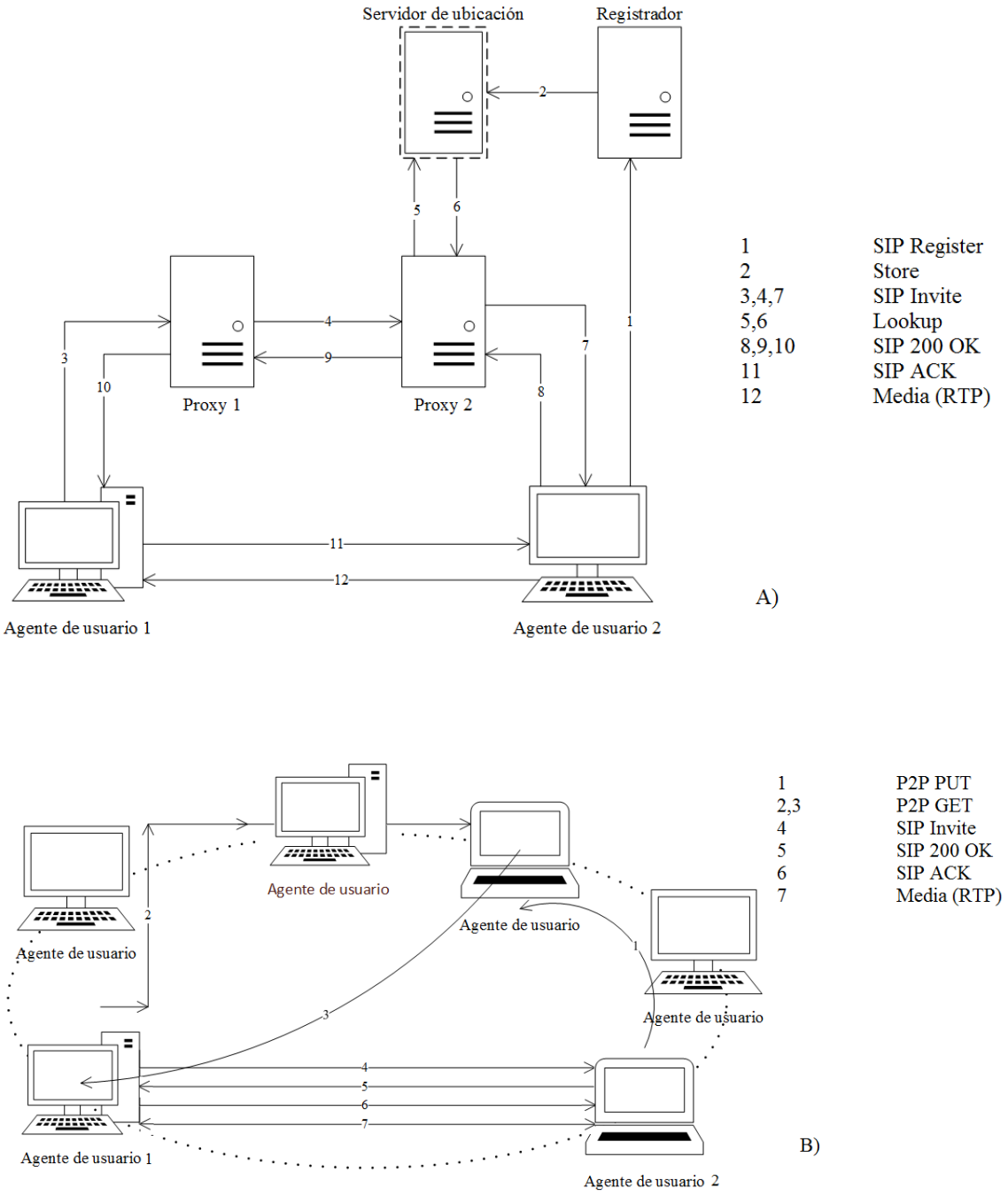


Figura 1.7. Flujo de mensajes para el establecimiento de una llamada entre el agente de usuario 1 y el agente de usuario 2 A) en SIP, B) en P2PSIP.

El protocolo RELOAD se desarrolló para brindar un servicio genérico para redes P2P, proporcionando mecanismos para el almacenamiento de objetos y para el enrutamiento de mensajes entre pares de la red sobrepuesta. Además de cumplir con las siguientes características requeridas dentro del ambiente P2P:

- Permite la utilización de RELOAD para diversas aplicaciones, ya que cuenta con una definición genérica de los tipos de datos y de las reglas de utilización de los mismos.
- Está diseñado para trabajar en ambientes donde los nodos se encuentran detrás de firewalls o NATs.
- Para minimizar la carga impuesta por el uso de nodos intermedios para las operaciones de enrutamiento, el encabezado de los mensajes es ligero.
- RELOAD brinda la capacidad de utilizar diversos algoritmos (topologías) para la red sobrepuesta, además de implementar Chord como topología default.
- Provee la opción de utilizar pares como clientes, es decir pares que no realizan las operaciones básicas dentro de la red sobrepuesta, como el almacenamiento de información o reenvío de mensajes en nombre de otros pares, sino que se limitan a almacenar su propia información dentro de la red sobrepuesta.
- Para enfrentar los riesgos que presentan las redes P2P en cuanto a seguridad, RELOAD brinda la opción de tener un servidor central encargado de autenticar a los nodos dentro de la red sobrepuesta.

1.5.2 Construcción básica

Una instancia de la red sobrepuesta de RELOAD consiste en un conjunto de nodos ordenados en un grafo parcialmente conectado. Cada nodo tiene asignado un identificador el cual junto con el algoritmo de la especificación determina la posición del nodo en el grafo, así como sus conexiones. Los algoritmos de las topologías de la red sobrepuesta deben asegurar que cualquier nodo tenga comunicación con cualquier otro nodo dentro de la red a pesar de que no se cuente con conexión directa y en un número limitado de saltos. Los pares en la red deben almacenar un conjunto de datos asociados a ciertas direcciones determinadas por el identificador de cada nodo.

1.5.3 Chord-RELOAD

La topología base para la red sobrepuesta de RELOAD es una adaptación del protocolo CHORD, las diferencias que presenta con respecto a este son:

- En Chord-RELOAD se incrementa la lista de sucesores y predecesores a más de uno por nodo.
- La tabla de dedos se indexa de manera inversa a Chord original, en este caso el dedo 0 es aquel que se encuentra a 180º del nodo origen, a diferencia del sucesor.
- El mecanismo de estabilización de la red puede llevarse a cabo de manera reactiva o de manera periódica. Esta facilidad permite realizar de manera eficiente los periodos de recuperación de la red, ante diferentes poblaciones.
- En el protocolo original se utiliza una función hash de 160 bits, sin embargo en esta adaptación se utilizan los 128 bits más significativos.
- Para mejorar la tolerancia ante fallas se almacenan réplicas en la lista de sucesores.
- Se utiliza una selección aleatoria para elegir dedos alternativos en caso de fallas: si el nodo tiene algún dedo inválido se reemplazará por uno nuevo con una probabilidad igual a 0.5, esto para minimizar el efecto debido al *churn*.

REFERENCIAS

[1] «Gnutella Protocol Development,» [En línea]. Available: http://rfc-gnutella.sourceforge.net/. [Último acceso: Agosto 2015].

[2] X. Shen, H. Yu y J. Buford, Handbook of Peer-to-Peer Networking, Springer, 2010.

[3] «BitTorrent,» [En línea]. Available: http://www.bittorrent.com/lang/es/. [Último acceso: Agosto 2015].

[4] B. Saleh y D. Qiu, «Performance Analysis of Network-Coding-Based P2P Live Streaming Systems,» *IEEE/ACM Transactions on Networking,* 2015.

[5] G. Zhang, W. Liu y X. Hei, «Unreeling Xunlei Kankan: Understanding Hybrid CDN-P2P Video-on-Demand Streaming,» *IEEE Transactions on Multimedia,* 2015.

[6] S. Li, W. Su y H. Li, «The Research of Security of P2P Network File Sharing System,» *IEEE 29th International Conference on Advanced Information Networking and Applications Workshops ,* 2015.

[7] M. Uruena, R. Cuevas, A. Cuevas y A. Banchs, «A Model to Quantify the Success of a Sybil Attack Targeting RELOAD/Chord Resources,» *IEEE Communications Letters,* 2013.

[8] D. Germanus, S. Roos, T. Strufe y N. Suri, «Mitigating Eclipse attacks in Peer-To-Peer networks,» *IEEE Conference on Communications and Network Security (CNS),* pp. 400-408, 2014.

[9] S. Diomidis y S. Androutsellis-Theotokhis, «A Survey of Content Distribution Technologies,» *ACM Computing Surveys,* 2004.

[10] J. F. Buford, H. Yu y E. K. Lua, P2P Networking and Applications, 2009.

[11] «The free network,» [En línea]. Available: https://freenetproject.org/. [Último acceso: Ago 2015].

[12] «The Language and Platform Independent Protocol for P2P Networking,» [En línea]. Available: https://jxta.kenai.com/. [Último acceso: Agosto 2015].

[13] «Skype,» [En línea]. Available: www.skype.com. [Último acceso: Agosto 2015].

[14] «The Statistics Portal,» [En línea]. Available: http://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/. [Último acceso: Agosto 2015].

[15] S. Baset y H. Schulzrinne, «An Analysis of the Skype Peer-to-Peer Internet Telephony Protocol,» Technical Report cucs-039-04, 2004..

[16] S. Guha, N. Daswani y R. Jain, «An experimental study of the Skype peer-to-peer VoIP,» IPTPS, 2006.

[17] «SopCast,» [En línea]. Available: http://www.sopcast.org/. [Último acceso: Agosto 2015].

[18] «PPS,» [En línea]. Available: http://www.pps.tv/. [Último acceso: Agosto 2015].

[19] H. Balakrishnan, M. Kaashoek, D. Karger, R. Morris y I. Stoica, «Looking up data in P2P systems,» *Communications of the ACM,* 2003.

[20] I. Stoica, R. Morris, D. Liben-Nowell, D. Karger, M. Kaashoek y F. Dabek, «Chord: a scalable peer-to-peer lookup service for Internet applications,» *IEEE/ACM Transactions on Networking,* 2003.

[21] S. Ratnasamy, P. Handley, R. Karp y S. Shenker, «A scalable content-addressable network,» *Proceedings of ACM SIGCOMM'01,* 2001.

[22] P. Maymounkov y D. Mazières, «Kademlia: A peer-to-peer information system based on the,» *Proceedings of 1st International Workshop on Peer-to-Peer,* 2002.

[23] A. Rowstron y P. Druschel, «Pastry: Scalable, distributed object location and routing for large-scale peer-to-peer systems,» *Proceedings of IFIP/ACM International Conference on Distributed Systems Platforms,* 2001.

[24] B. Zhao, L. Huang, J. Stribling, S. Rhea, A. Joseph y J. Kubiatowicz, «Tapestry: A resilient global-scale overlay for service deployment,» *IEEE Journal on Selected Areas in Communications,* 2004.

[25] D. Karger, E. Lehman, T. Leighton, M. Levine, D. Lewin y R. Panigrahy, «Consistent hashing and random trees: distributed caching protocols for relieving hot spots on the World Wide Web,» *Proceedings of the twenty-ninth annual ACM symposium on Theory of computing,* 1997.

[26] C. Jennings, B. Lowekamp, E. Rescorla, S. Baset y H. Schulzrinne, «REsource LOcation And Discovery (RELOAD),» *Rfc 6940,* 2014.

[27] R. Schollmeier, «A definition of peer-to-peer networking for the classification of peer-to-peer architectures and applications,» *Peer-to-Peer Computing,* 2001.

[28] D. Germanus, *Increasing Structured P2P Protocol Resilience to Localized Attacks,* Technische Universität, Darmstadt, 2015.

CAPÍTULO 2

2. SEGURIDAD EN REDES SOBREPUESTAS *PEER-TO-PEER*

En este capítulo se introducen las nociones básicas sobre la seguridad en redes P2P, particularmente en las redes sobrepuestas del tipo estructurado. Se tratan los requerimientos que los sistemas P2P en cuanto a seguridad se refiere. Además, se presentan de manera general los principales ataques y sus respectivas defensas que afectan a las redes sobrepuestas P2P. Para finalizar, se revisa el modelo de seguridad del actual protocolo de señalización normalizado por [1], para las redes *Peer-to-Peer*, RELOAD.

2.1 INTRODUCCIÓN

Hoy en día, diversos servicios que se cursan sobre Internet como son: el almacenamiento de información en la nube, el manejo y administración de los recursos financieros, tanto personales como corporativos; recaen sobre la certeza de que estos sean robustos ante eventualidades de fallo y, aún más, ante posibles ataques de seguridad. Con la creciente aparición de nuevos tipos de ataques, desde *virus*, *adware*[2], *spyware*[3], denegación de servicio[4], hasta fraude o suplantación

[2] Tipo de software, donde de manera automática exhibe al usuario anuncios publicitarios.
[3] Tipo de software malicioso que accede a los datos de una computadora y los envía a otros dispositivos sin que el usuario lo advierta.
[4] Ataque a un sistema de computadoras, o red, que causa que un servicio o recurso sea inaccesible a los usuarios legítimos del mismo.

de identidad, el asegurar la confiabilidad de un sistema resulta de gran importancia en un entorno donde todas las operaciones diarias se apoyan en mayor o menor medida en Internet.

Sin una autoridad central que verifique la autenticidad de los usuarios dentro de la red y la integridad de los datos, los sistemas P2P imponen nuevos desafíos para hacer prevalecer la seguridad. Debido a las cualidades de los sistemas P2P como lo son la autonomía y su naturaleza abierta, el ambiente P2P presenta nuevos obstáculos para asegurar la confiabilidad de los datos. Por ejemplo, ante el usual movimiento de entrada y salida de nodos en la red, si éste continúa incrementándose puede resultar en un ataque potencial de negación de servicio causado por el aumento de tráfico de control y mantenimiento de la red. Asimismo, si los nodos dentro de la red no se comportan de acuerdo a lo establecido por los protocolos del sistema, es decir modifican los procedimientos de envío de mensajes o de almacenamiento, etc., se puede llevar al límite de seguridad a la red P2P sobrepuesta por un comportamiento inesperado.

En la actualidad las aplicaciones implementadas sobre redes P2P como la compartición de archivos P2P, el *streaming* de información multimedia P2P, P2PTV o los juegos P2P, proporcionan nuevas plataformas de acción a los criminales cibernéticos para obtener información confidencial, alterar documentos, contenido o inclusive dispositivos, entre otros intentos criminales de índole doloso [2], [3].

2.1.1 Requerimientos de seguridad en una red P2P.

De acuerdo con las recomendaciones del Sector de Normalización de Telecomunicaciones de la Unión Internacional de Telecomunicaciones (ITU-T, *ITU Telecommunication Standardization Sector*) [4] en un sistema P2P se tienen los siguientes requerimientos de seguridad:

- Autenticación del usuario. Se utiliza para demostrar la identidad de los pares dentro la red.
- Anonimato. En algunas aplicaciones es deseable que los usuarios permanezcan anónimos durante la comunicación P2P, lo que permite mayor accesibilidad a la red. Sin embargo,

el anonimato también provee facilidades para atacar la seguridad dentro de una red P2P, por lo que es necesario brindar seguridad propia a este requerimiento.

- Privacidad. Se refiere a brindar protección a aquella información que podría obtenerse de la observación de las actividades o de la comunicación en la red, por ejemplo el contenido de los mensajes, la localización de los usuarios, etc.
- Integridad de datos. Debido a que en los sistemas P2P la información se distribuye entre todos los pares dentro de la red y se dirige a través de pares intermedios, si existen nodos maliciosos en la red, estos pueden modificar los datos. La integridad de datos asegura que se reciban correctamente los datos o los mensajes enviados, es decir, éstos se protegen contra la alteración, creación, eliminación o replicación no autorizada.
- Confidencialidad de los datos. En algunos casos, los usuarios desean que los datos o mensajes que se transmiten por la red no puedan ser leídos por pares no autorizados.
- Control de acceso. Éste se refiere a la protección contra el acceso no autorizado a cierto tipo de recursos, asegurando que sólo usuarios permitidos puedan obtener cierta información o enviar mensajes. Además, se restringe el acceso a la red a usuarios sin los criterios establecidos o la comunicación entre usuarios sin las credenciales necesarias.
- No repudio. El no repudio puede utilizarse para demostrar el origen de los datos, es decir, para verificar que los datos provienen de un par en particular, para evitar la negación de las actividades de los pares. Asimismo, el no repudio puede utilizarse para demostrar la entrega de los datos, para impedir que haya negación en la recepción de datos o mensajes.
- Usabilidad. Para evitar problemas de seguridad, las aplicaciones P2P deben proveer de interfaces de usuario y mecanismos de seguridad que no permitan que usuarios mal intencionados modifiquen la configuración de los procedimientos establecidos dentro del sistema P2P.
- Disponibilidad. Se debe asegurar la disponibilidad de los datos ante posibles eventos que afecten a la red, es decir, los datos deben estar disponibles cuando sean requeridos a pesar de fallos o ataques en el sistema. Además, se debe asegurar que las aplicaciones puedan proporcionar el servicio en cualquier momento.
- Control de tráfico. Cuando existe congestión en la red, los sistemas P2P deben ser capaces de mitigar sus consecuencias.

En el caso de redes de telecomunicaciones basadas en P2P, como por ejemplo para el servicio de voz sobre IP y para el *streaming* de datos multimedia, los requerimientos de seguridad recomendados son [5]:

- Autenticación y autorización. La identidad de todos los nodos dentro de la red debe poder ser validada remotamente, además, los recursos y servicios deben ser propiamente autorizados.
- Manejo de confianza. El ambiente abierto que proveen las redes P2P propicia que los nodos maliciosos dañen la comunicación entre pares o al sistema en sí, por lo que se requieren de mecanismos de confianza para determinar de manera remota si un nodo es confiable y hasta qué punto lo es, para realizar los procesos y operaciones dentro del sistema.
- Confidencialidad. En el caso de la voz sobre IP, la confidencialidad provee mecanismos para evitar la intercepción de las conversaciones y mensajes de señalización entre los participantes. Dentro del servicio de *streaming*, información clave de los usuarios puede ser dirigida y temporalmente almacenada por nodos intermedios, debido a lo cual, la señalización, el perfil de usuario y el contenido multimedia deben ser protegidos.
- Integridad. La integridad de los mensajes y de los paquetes de datos en una conversación de voz sobre IP es de vital importancia, ya que los atacantes pueden alterar los paquetes o modificar los mensajes de señalización, resultando inclusive en llamadas fallidas. En el servicio de *streaming,* durante la fase de establecimiento se pueden modificar los datos generando ataques de negación de servicio o resultando en que el usuario termine con archivos incorrectos.

Las operaciones básicas dentro de una red P2P también deben protegerse con mecanismos de seguridad como se detalla a continuación [6]:

- Unión a la red. Si no existen limitaciones en la unión de pares en la red, éstas pueden resultar vulnerables. Por esta razón, se requieren de mecanismos que aseguren la autenticación de los usuarios, que brinden anonimato de tal forma que un observador externo no pueda obtener información de los pares dentro de la red, así como la revelación no deseada de información personal del usuario hacia los demás usuarios dentro de la red.

- Salida de la red. Para evitar una desestabilización en el funcionamiento de la red, es necesario que se implementen mecanismos de notificación de salida seguros, evitando la filtración de información sensible del usuario que abandona la red, así como asegurando la integridad de los datos y conexiones que cede.
- Búsqueda dentro de la red. Las operaciones de búsqueda pueden o no estar restringidas para un determinado grupo de pares del sistema de acuerdo con los requerimientos de la aplicación P2P. Además, se debe proporcionar seguridad a los que realizan y contestan una búsqueda, de tal forma que observadores externos no puedan obtener información significativa de los participantes. Asimismo, se debe mantener la integridad de los mensajes para prevenir la manipulación maliciosa, ya que los pares intermedios podrían realizar ataques de negación de servicio o de fallas simuladas en la búsqueda. Los datos resultantes de una búsqueda también pueden requerir autorización para ser obtenidos por los usuarios, adicionalmente, debe limitarse su demanda para evitar congestionamientos en la red o posibles ataques de negación de servicio.
- Enrutamiento. Los mecanismos de enrutamiento pueden conllevar a una autenticación de los usuarios si el servicio lo requiere, además de requerir que se mantenga la integridad de los mensajes y evitar la propagación de información sensible de los nodos dentro de la ruta, así como el no repudio de los participantes.
- Operaciones de inserción y obtención de datos. Estas operaciones deben cuidar el acceso a los datos por medio de políticas de autenticación y de control de acceso.
- Operaciones de actualización y eliminación de datos. Se deben implementar mecanismos de autorización de estas operaciones, así como de no repudio o trazabilidad.

2.2 ATAQUES A LAS REDES P2P

2.2.1 Introducción

Los diversos ataques que se pueden realizar en los sistemas P2P se pueden clasificar de acuerdo a diferentes criterios, a continuación se hace una clasificación general [7] y posteriormente una detallada de los ataques.

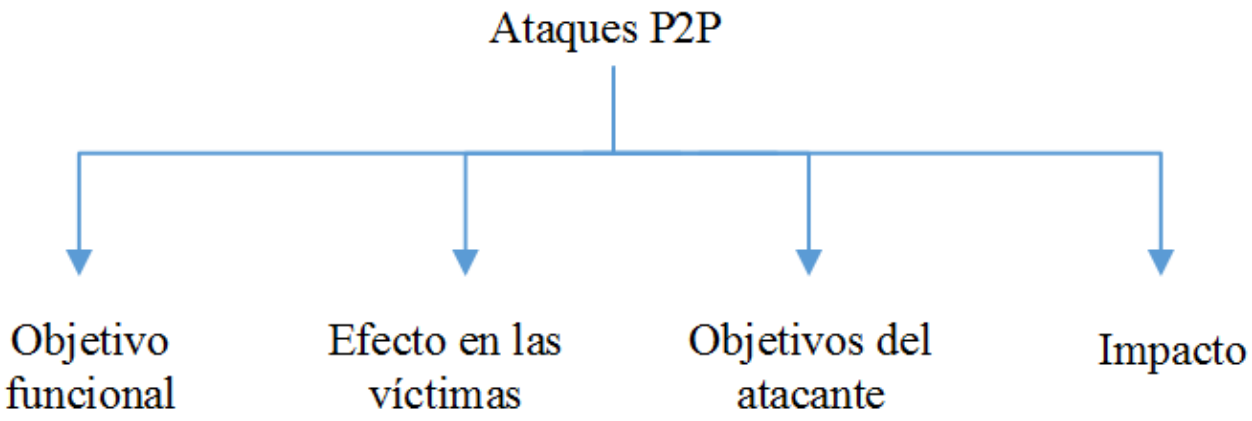


Figura 2.1. Clasificación general de los ataques en los sistemas P2P.

Objetivo Funcional.

Los ataques en los sistemas P2P pueden estar enfocados a las diferentes capas del sistema, ya sea a la capa de aplicación, la de la red sobrepuesta o la red subyacente. La seguridad de cada capa depende de las garantías de seguridad que provee la capa inmediata inferior.

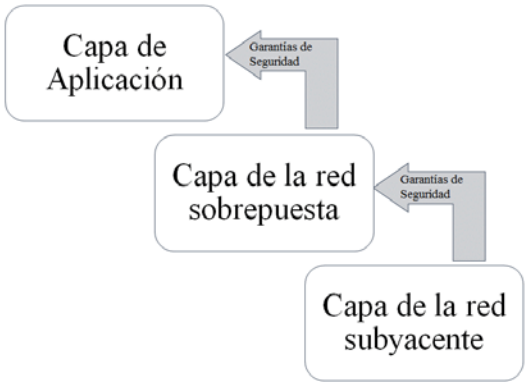


Figura 2.2. Ataques por objetivo funcional.

Los ataques en la capa de aplicación están directamente relacionados con la interacción con el usuario a través de las interfaces de usuario del servicio que ofrece el sistema. En la red sobrepuesta, los ataques están ligados con las operaciones básicas dentro de la red, por ejemplo: en el enrutamiento de mensajes o el almacenamiento de los objetos. El estudio de seguridad que se realiza en esta tesis se limita al referente a redes sobrepuestas estructuradas. Finalmente, los ataques realizados sobre la red subyacente son aquellos enfocados a la manipulación e intercepción de los paquetes o al enrutamiento erróneo de los mismos.

Efecto en las víctimas.

Los mensajes dentro de la red sobrepuesta son susceptibles a los siguientes ataques:

- Interrupción no autorizada.
- Intercepción o acceso no autorizado.
- Modificación o alteración no autorizada.
- Creación no autorizada.

Estos ataques pueden ser del tipo activo o pasivo, por medio de la comunicación entre pares o a través de mecanismos de ataque embebidos (virus, troyanos, etc.). El espionaje, substitución o inserción, la interferencia, la sobrecarga, el análisis criptográfico, la escucha no autorizada y la negación de servicio son ejemplos de este tipo de ataques.

Objetivos del atacante.

Los objetivos del atacante se clasifican en activos, como por ejemplo, el robo de información o de recursos, manipulación de los dispositivos e inclusive de la red completa y la interrupción de los servicios ofrecidos. Así como también pueden clasificarse en objetivos pasivos, que pueden ser el análisis del tráfico o de las señales en el sistema.

Impacto

El impacto de un ataque se refiere a si este tiene como consecuencia un efecto disruptivo, en particular de los servicios proporcionados por el sistema, o a una degradación de la calidad de los mismos.

2.2.2 Ataque Sybil.

La idea detrás de este ataque [8] es que una entidad maliciosa presenta identidades múltiples, con las cuales adquiere responsabilidad sobre diversos recursos y control sobre algunas porciones de la red. Aún más, si el atacante es capaz de posicionar sus identidades ficticias en posiciones estratégicas dentro de la red, el daño que puede lograrse es considerable.

El que una entidad maliciosa presente identidades múltiples es un mecanismo mediante el cual se pueden llevar a cabo distintos ataques, es decir, si se cuentan con un número significativo de identidades falsas el ataque puede realizarse a nivel almacenamiento de los datos, en el enrutamiento o en el servicio.

Sin la presencia de una autoridad que confirme la correspondencia entre una entidad y una identidad, a una entidad le será siempre posible presentar identidades múltiples. Además, la habilidad de un par de distinguir a nodos remotos y sus identidades depende de la primicia de que los recursos de un ataque son limitados, por lo que su validación podría hacerse enviándole desafíos para contabilizar sus recursos. Sin embargo, para que esta validación fuera efectiva, se requiere que: todos los pares dentro de la red tengan un número de recursos parecido, que todas las identidades se validen de manera simultánea por todos los pares y que cuando se acepten identidades indirectamente[5], que el número de identidades que se validan sea mucho mayor a las del número de fallas global. En un ambiente P2P es difícil cumplir con estos requerimientos, por lo que actualmente las soluciones para contratacar la creación de identidades Sybil son [9]:

[5] La validación indirecta es aquella en la cual un nodo local acepta la validación remota que realizan un conjunto de nodos que se encuentran dentro de su conjunto de nodos validados.

- La utilización de desafíos computacionales. Cada nodo en la red resuelve un desafío computacional cuando quiere acceder a la red y después de cierto intervalo de tiempo se vuelve a evaluar de nuevo, haciendo que para un usuario malicioso sea costoso tener identidades múltiples. Sin embargo, esta solución sólo es válida para sistemas donde el número de recursos por nodo en la red es similar.
- Limitación de los recursos humanos. Con la utilización de CAPTCHA (*Completely Automated Public Turing test to tell Computers and Humans Apart*) se puede proteger de *bots*[6] en la red, asegurando que cada operación dentro del sistema está realizada por un humano. Sin embargo, en una red P2P muy grande es poco práctico evaluar a cada uno de los nodos con los que se interactúa.
- Modelos de confianza. En estos sistemas cada nodo tiene asignado niveles de confianza a cada par con el que ha interactuado directamente, los cuales pueden utilizarse para evaluar de manera indirecta a otros pares. No obstante, esto no previene que una entidad cree múltiples identidades, sólo las califica.
- Redes sociales. Basándose en el hecho que las identidades Sybil están fuertemente conectadas entre sí, al provenir de una misma entidad, pero escasamente conectadas con los demás nodos en la red, con lo cual se pueden detectar las actividades sospechosas para limitar su número.
- Control centralizado. La forma más fácil de establecer medidas contra la aparición de identidades Sybil es mediante el uso de una entidad certificadora centralizada que asocie certificados con identidades, ya sean identidades en el mundo real o por medio de cuotas de admisión. Ésta es la forma de acceso presentada en el protocolo RELOAD [1].

  Aunque esta solución resuelve de manera más completa el problema de las identidades múltiples Sybil, presenta ciertas restricciones. La entidad centralizada es un punto de ataque único además de que actúa como un cuello de botella ante una gran cantidad de peticiones. Adicionalmente, puede existir un incremento en el costo de las comunicaciones ya que al realizar una transacción entre dos pares podría ser necesario validar primero con la autoridad. Por último, la entidad de control centralizado debe

[6] Tipo de software malicioso que permite a un atacante tomar el control de un equipo infectado o que es capaz de llevar a cabo tareas concretas e imitar el comportamiento humano.

diseñarse para ser escalable y confiable, especialmente para aplicaciones que incluyen un gran número de usuarios de diferentes capacidades y procedencias.

La mayor amenaza que presenta el mecanismo de creación de identidades Sybil depende de los objetivos del atacante. Como específica [10], si el objetivo del atacante es el aislamiento de un objeto en particular, en una red donde la asignación de identificadores se hace de manera aleatoria como en Chord-RELOAD, con un tamaño de red de 4 millones de usuarios y con un factor de replicación de los objetos igual a 10, el atacante debería generar 55.7 millones de identidades para obtener una probabilidad del 0.5 de éxito. Sin embargo, si el objetivo del atacante es degradar la calidad del servicio de los usuarios dentro de la red, podría hacer que sus identidades retrasaran la búsqueda, degradar el almacenamiento o los servicios de enrutamiento sin la necesidad de crear una cantidad de identidades tan grande.

2.2.3 Ataques en el procedimiento de enrutamiento

Debido a que los servicios que brindan las aplicaciones P2P se sostienen sobre una red sobrepuesta, ésta introduce un requerimiento de seguridad adicional que debe considerarse. Uno de los servicios básicos que proporciona la red sobrepuesta es el servicio de enrutamiento de mensajes dentro de la red P2P, en la cual nodos intermedios dirigen los mensajes desde un nodo origen a un nodo destino de acuerdo con la topología de la red sobrepuesta estructurada por medio de un criterio de cercanía determinado. En estos sistemas es de vital importancia asegurar la exactitud en las funciones de búsqueda, aún ante la presencia de nodos maliciosos que actúan de manera activa en el sistema, es decir, no sólo en el enrutamiento sino también pueden proporcionar información alterada a los nodos en la fase de actualización.

Los ataques en el procedimiento de enrutamiento pueden clasificarse en [11]:

- Enrutamiento de búsqueda incorrecto.
- Incorrecta actualización del enrutamiento.
- Partición de la red.

Enrutamiento de búsqueda incorrecto

En este tipo de ataque el nodo malicioso dirige las búsquedas hacia un nodo incorrecto o uno no existente. Dado que el nodo malicioso participa de manera normal en la fase de actualización de la red sobrepuesta, éste no es removido de las tablas de enrutamiento de los demás nodos, por esta razón, las retransmisiones de las búsquedas se continúan enviando al nodo malicioso.

Debido a la construcción de las redes sobrepuestas estructuradas donde las búsquedas están determinadas por un número finito de saltos dado, el enrutamiento mal dirigido puede detectarse al verificar que con cada salto en la búsqueda se acerca al destino, es decir, la distancia disminuye con cada salto. El nodo origen debe verificar que se está realizando de manera correcta la búsqueda revisando cada salto de progreso de esta, de lo contrario podría determinar el nodo que está actuando malintencionadamente e intentar otras alternativas de búsqueda.

Otra forma de detectar este ataque es iniciar búsquedas de manera aleatoria para verificar la validez de las rutas. No obstante, si el nodo origen se encuentra lejano, no podrá determinar si la búsqueda realmente lo está llevando más cerca al recurso destino o no. Para evitar estos ataques, además de requerir un proceso de verificación de la distancia restante, es necesario que los objetos sean asignados a los nodos de manera verificable. Por ejemplo, en el caso de que los objetos sean asignados a los nodos cercanos dentro del espacio de identificadores, entonces para que la asignación de llaves sea verificable, la asignación de los nodos debe ser verificable.

Actualización del enrutamiento incorrecta.

Dado que cada nodo en el sistema construye su tabla de enrutamiento de acuerdo con la información que recibe de otros nodos, un nodo malintencionado podría contaminar las tablas de enrutamiento de los demás nodos si envía información incorrecta. Las actualizaciones incorrectas podrían ocasionar que los nodos dirijan de manera errónea la búsqueda a nodos no apropiados o no existentes. Sin embargo, si el sistema tiene conocimiento de los requerimientos que las entradas de actualización deben cumplir, es posible detectar cuando se tienen comportamientos maliciosos. Por ejemplo, si se sabe que los nodos deben cumplir con cierto

prefijo, o estar dentro de un determinado rango, etc. Otra posible solución es el envío de tablas de enrutamiento redundantes, en donde cada nodo envía su tabla de enrutamiento de manera aleatoria o periódica a sus vecinos y nodos con conexión directa, el nodo que recibe las tablas las coteja y determina cuáles entradas son de riesgo y cuáles no. Por último, se han implementado soluciones de monitoreo, centralizadas y distribuidas, donde los monitores de la red cuidan que se preserve la integridad de las actualizaciones.

Partición de la red.

Cuando un nuevo nodo accede al sistema debe ponerse en contacto con un nodo *bootstrap*[7], el cual lo asiste colocándolo en su posición dentro del espacio de identificadores. Sin embargo, el nodo nuevo es vulnerable a que sea introducido a una red incorrecta. Suponiendo que existe un conjunto de nodos maliciosos que forman una red paralela a la ya existente, que ejecuta los mismos procedimientos que la red legítima, totalmente consistente y pudiendo contener información legítima de la red, entonces el nodo podría unirse a esta red accidentalmente y obtener resultados incorrectos en sus operaciones. Asimismo, un nodo malicioso puede hacer que algunos nodos se conecten a esta red aún si estos cuentan con un *bootstrap* válido de manera paulatina.

Las particiones se pueden utilizar para negar servicios o para obtener información sobre el comportamiento de algunos pares que de alguna otra forma resultaría más complejo. Por ejemplo, si el servicio brindará algún tipo de anonimato en las transacciones (publicaciones o interacciones), los nodos maliciosos podrían rastrear las identidades de quienes leen o almacenan datos a través de una partición.

Para evitar que un nodo sea introducido en una red incorrecta, es necesario que el nodo *bootstrap* al que accede sea una fuente confiable, pudiendo ser una entidad centralizada fuera o no de línea. Además, si el nodo ya había estado en la red previamente puede utilizar nodos conocidos en anteriores conexiones para realizar su proceso de unión o para verificar si la red es correcta o una partición, por medio de búsquedas aleatorias con su tabla de enrutamiento actual y alguna

[7] Nodo de control del ingreso.

previamente construida. Por último, si el nodo no cuenta con un conocimiento previo de la red, podría realizar búsquedas aleatorias y realizar mecanismos de seguimiento para verificar que no se encuentra dentro de una partición.

Enrutamiento seguro en una red sobrepuesta estructurada P2P

En [12] se fundaron los principios para tener un enrutamiento seguro:

- Asignación segura de identificadores. Asegura que un nodo malicioso no pueda elegir el identificador que le corresponde y que una coalición de nodos maliciosos no pueda escoger un conjunto de identificadores de manera ilegítima, de tal forma que puedan controlar el acceso a un recurso o que incrementen la probabilidad de controlar las rutas de un nodo determinado.
- Mantenimiento seguro de las tablas de enrutamiento. Asegura que se disminuyan las entradas erróneas en la tabla de enrutamiento de un nodo, para lo cual se sugiere que se establezcan restricciones sobre el conjunto de nodos que pueden llenar las entradas en la tabla de enrutamiento.
- Reenvío de mensajes seguro. Asegura que un mensaje no sufra modificaciones mientras se transmite entre los nodos intermedios pudiendo sufrir alteraciones o desviaciones, asegurando que al menos una copia del mensaje llegue al nodo destino con alta probabilidad.

Las soluciones a estos principios dependen de la aplicación o el servicio que proporciona la red sobrepuesta y de sus limitantes.

2.2.4 Ataques en los procedimientos de almacenamiento y obtención de información.

Los sistemas P2P que se utilizan como depósitos de información distribuidos pueden sufrir los siguientes ataques en los procedimientos de almacenamiento y obtención de datos:

- Un nodo malicioso puede rehusarse a almacenar la información de la que es responsable.
- El nodo puede acceder a almacenar la información para posteriormente eliminarla.

- El nodo puede hacerse responsable de la información, pero no la otorga a los nodos que la solicitan o puede devolver una copia alterada de la información.
- El nodo puede actuar de manera conjunta y coordinada con otros atacantes.
- El nodo se puede hacer pasar por otro nodo.
- El nodo puede acceder a la información que está almacenando.

Estos ataques también se aplican a sistemas donde se almacena meta información, por ejemplo el almacenamiento de información de enrutamiento.

La principal solución a estos ataques es el almacenamiento redundante [13], es decir, al objeto se le generan copias que son almacenadas en varios nodos responsables, de esta manera si alguno de los nodos dentro del conjunto de nodos responsables es malicioso es posible encontrar el objeto en los demás nodos restantes. No obstante, aunque esta solución permite disminuir los ataques a los procedimientos de almacenamiento y obtención de los datos, trae consigo un compromiso entre el número de copias que se deben almacenar y el tráfico y complejidad que su búsqueda conllevan. Para evitar que un nodo niegue la responsabilidad de algún objeto previamente almacenado o que la elimine, se utilizan certificados de responsabilidad que asocian el identificador del objeto con el nodo responsable. Además, los certificados permiten verificar la integridad del objeto al incluir el contenido del mismo en la asociación.

En algunas aplicaciones, la información que se almacena puede tener contenido privado, por lo que es necesario proporcionar mecanismos para que sólo nodos autorizados puedan almacenar o acceder a la información. Estos mecanismos pueden realizarse por medio de funciones criptográficas, ya sea de llave privada o llave pública, así como por entidades de control que almacenan los objetos o que supervisan el almacenamiento.

2.2.5 Ataques de Negación de Servicio.

En una red P2P los nodos participantes deben estar disponibles en cualquier momento para poder contribuir con la información de la que son responsables o para participar en los procedimientos de búsqueda y enrutamiento. Sin embargo, un nodo puede volverse no disponible si es víctima de un ataque de negación de servicio. En estos ataques, el nodo se

sobrecarga con una gran cantidad de mensajes o peticiones, de tal forma que se encuentra ocupado atendiendo un gran número de solicitudes insignificantes que consumen sus recursos evitando que cumpla con sus actividades dentro de la red.

Los ataques pueden darse a nivel de la red sobrepuesta o a nivel de la aplicación. Los ataques sobre la red sobrepuesta intentan invalidar un nodo por medio de una inundación de mensajes, es decir, de tráfico, mientras que los ataques de negación de servicio a nivel de aplicación lo intentan por medio de peticiones.

Las soluciones a este tipo de ataques se pueden dividir en 3 etapas:

- Detección del ataque. En esta etapa se evalúa al nodo para determinar si se encuentra bajo un ataque de sobrecarga de peticiones o mensajes.
- Manejo del ataque. El manejo de los ataques de negación de servicio usualmente se realiza mediante el balanceo de carga entre todos los nodos en la red; es decir, sin importar la cantidad de mensajes o peticiones que el nodo debería contestar, siempre dedica una cantidad fija de recursos a cada nodo. La cantidad de recursos asignados a cada nodo puede ser proporcional entre todas las peticiones que soporta el nodo o fraccionaria, repartiendo las peticiones de manera equitativa.
- Recuperación del ataque. En esta etapa el nodo se desvincula de los nodos maliciosos, pudiendo enviar notificaciones a sus conocidos.

2.2.6 Ataques a la información almacenada.

Debido a que los sistemas P2P proporcionan ambientes abiertos, pueden introducirse nodos maliciosos a la red que pueden corromper la información que almacenan, reemplazarla o inclusive entregarla incompleta. Mientras que para el dueño de la información puede ser fácil verificar que ésta se encuentra en estado correcto, no resulta así para los nodos que podrían requerirla en alguna búsqueda.

La solución directa sería sólo almacenar información en nodos autorizados o confiables, que hayan sido acreditados por alguna autoridad confiable dentro del sistema. Sin embargo, esta solución además de traer consigo un incremento de carga sobre estos nodos, limita la aplicación

de los sistemas P2P. La solución sería entonces no depender de ningún nodo confiable, sino que la verificación se hiciera sobre el objeto que se requiere en las búsquedas. Esta verificación debe tener las siguientes propiedades:

- Debe permitir verificar que los objetos que entrega el nodo no confiable sean parte del conjunto de objetos respuesta de la petición.
- Debe permitir verificar que el objeto está completo.

La solución común a estos ataques es mediante el uso de funciones criptográficas de firma y verificación de los datos, por medio del uso de certificados asociados a cada objeto dentro de la red. Sin embargo, la solución está ligada a los requerimientos de la aplicación o servicios que brinda el sistema P2P.

2.3 SEGURIDAD EN RELOAD.

2.3.1 Introducción.

El actual protocolo de señalización para sistemas P2P de la IETF, RELOAD [1], define un modelo de seguridad genérico aplicable a los usos de RELOAD.

> El objetivo del modelo de seguridad de RELOAD es proporcionar fuertes garantías de seguridad en ciertas propiedades de la red sobrepuesta aún con la presencia de una gran cantidad de nodos maliciosos, y permitir que la red sobrepuesta funcione correctamente bajo la presencia de una cantidad modesta de nodos maliciosos.

Debido a que los servicios básicos que proporciona RELOAD son el almacenamiento y enrutamiento, los mecanismos de seguridad establecidos se centran en estos servicios. En RELOAD, un par es responsable de almacenar la información de un nodo de la red y además permite a nodos terceros obtener esta información, mientras que otros nodos se encargan de enrutar mensajes desde y hacia los nodos que almacenan la información.

En el protocolo se especifican estrategias de seguridad basadas en certificados que protegen la información de los usuarios y el enrutamiento de nodos subversivos que podrían intentar dirigir erróneamente el enrutamiento, alterar o eliminar los objetos almacenados, o espiar las transacciones entre los pares del sistema.

Para la protección contra atacantes externos que pretenden ser usuarios válidos o algún otro nodo ya existente, todas las comunicaciones se realizan mediante canales seguros TLS (*Transport Layer Security*) o DTLS (*Datagram Transport Layer Security*) que proveen integridad en los mensajes y autenticación de los participantes. Adicionalmente, todos los mensajes y objetos deben ser firmados digitalmente con la firma pública del remitente, para proporcionar seguridad extremo-extremo.

2.3.2 Utilización de certificados en RELOAD.

El modelo de seguridad en RELOAD está basado en que cada entidad dentro del sistema autentique criptográficamente mediante un par de llaves, pública y privada, ligadas en un certificado. Este modelo proporciona seguridad a los datos en la red sobrepuesta y a su enrutamiento.

En el momento de unión a la red, el usuario solicita a la entidad autorizada de registro, un nombre único y uno o varios identificadores dentro del espacio de identificadores, los cuales se asocian a un certificado con la llave pública del usuario. La entidad que firma todos los certificados de los usuarios de la red actúa como una entidad certificadora, permitiendo verificar los certificados de los nodos sin que estos se comuniquen directamente puesto que todos obtienen la llave pública de esta autoridad certificadora cuando se registran en la red.

En RELOAD también se presenta la posibilidad de utilizar un mecanismo de auto-certificación o uno de llave compartida, los cuales pueden ser apropiados para redes pequeñas donde todos los usuarios sean confiables.

Para verificar que un nodo cuenta con las credenciales para realizar un almacenamiento en la red se recurre al certificado del nodo dueño de la información, en este se confirma si cuenta con la autorización. Además, debido a que toda la información está firmada digitalmente por su dueño,

los nodos que la obtienen de la red pueden comprobar que ésta se encuentra integra y revisar su origen.

2.3.3 Seguridad en los procedimientos de almacenamiento

El modelo de seguridad en RELOAD basado en certificados proporciona las siguientes características:

- Autorización de almacenamiento. Cuando un nodo quiere guardar un objeto en la red sobrepuesta debe primero firmarlo con su llave privada y posteriormente el responsable de almacenarlo debe comprobar que el usuario tiene permitido almacenar ese tipo de objeto, de acuerdo con las políticas de acceso del sistema.
- Límites en el almacenamiento. Cada tipo de objeto que se almacena en un nodo tiene asociado un conjunto de certificados, entre ellos se encuentra definido un límite máximo de objetos a almacenar. Esta limitación permite no sobrecargar a los nodos responsables, así como la realización de posibles ataques de negación de servicio.
- Integridad de los datos. Por medio de la verificación de la firma digital de cada dato se puede comprobar su integridad.

2.3.4 Seguridad en los procedimientos de enrutamiento

En general, los ataques a los procedimientos de enrutamiento dentro de una red sobrepuesta se basan en que el atacante logre dirigir el tráfico a través de nodos que él controla [14]. No obstante, para lograr el control sobre los nodos deseados es necesario que pueda manipular los identificadores de estos. En RELOAD esto no es posible debido a que la asignación de identificadores se hace por medio de una entidad centralizada que los asigna de manera aleatoria. Además, en el protocolo se proporcionan otras características en el modelo de seguridad referentes a los procedimientos de enrutamiento:

- Autenticación en las conexiones directas. Cuando un par se quiere comunicar con otro par, previamente cada uno verifica que el otro tenga posesión de un certificado adecuado, correspondiente al nodo con quien cree realizar la conexión.

- Establecimiento de canales seguros en las conexiones directas. Una vez verificada la identidad de los nodos que intervienen en la conexión, todos los mensajes entre estos viajan a través de un canal seguro TLS o DTLS. Este canal protege la información de atacantes externos a la red sobrepuesta.
- Integridad de los mensajes. Para evitar que nodos intermedios en la ruta de enrutamiento alteren el contenido de los mensajes, estos se firman digitalmente, permitiendo que los nodos destino verifiquen su integridad.
- Autenticación del origen. Aun cuando algún nodo no está conectado de manera directa es posible comprobar su identidad di genera un mensaje, ya que todos los mensajes de enrutamiento dentro de la red están firmados por el par que los formó.
- Limitación en el número de saltos. Para evitar posibles ataques de enrutamiento cíclico cuando se utiliza el procedimiento de enrutamiento de lista origen (*source routing*), donde un nodo especifica aquellos nodos por los que desea que un mensaje pase en una búsqueda, se limitan el número de saltos que se realizan para llevar a cabo la búsqueda. El valor de este límite está dado por el máximo número de saltos en la red sobrepuesta, éste depende de la topología de la misma y del número de nodos esperado o máximo en el sistema.

REFERENCIAS

[1] C. Jennings, B. Lowekamp, E. Rescorla, S. Baset y H. Schulzrinne, «REsource LOcation And Discovery (RELOAD),» *Rfc 6940,* 2014.

[2] «Tiversa,» [En línea]. Available: http://www.tiversa.com/learningcenter/resources/keyconcepts/. [Último acceso: 2015].

[3] F. Adamsky, S. A. Khayam, R. Jäger y M. Rajarajan, «P2P File-Sharing in Hell: Exploiting BitTorrent Vulnerabilities to Launch Distributed Reflective DoS Attacks,» *24th USENIX Security Symposium,* 2015.

[4] *ITU-T Recommendation X.1161, Framework for secure peer-to-peer communications,* 2009.

[5] *ITU-T Recommendation X.1163, Security requirements and mechanisms of peer-to-peer-based telecommunication networks,* 2015.

[6] *ITU-T Recommendation X.1162, Security architecture and operations for peer-to-peer networks,* 2009.

[7] J. F. Buford, H. Yu y E. K. Lua, P2P Networking and Applications, 2009.

[8] J. R. Douceur, « The Sybil attack,» *IPTPS '01: Revised papers from the 1st international,* 2002..

[9] D. Touceda, J. Sierra, A. Izquierdo y H. Schulzrinne, «Survey of Attacks and Defenses on P2PSIP Communications,» *Communications Surveys & Tutorials, IEEE,* 2012.

[10] M. Uruena, R. Cuevas, A. Cuevas y A. Banchs, «A Model to Quantify the Success of a Sybil Attack Targeting RELOAD/Chord Resources,» *Communications Letters, IEEE,* 2013.

[11] Q. H. Vu, M. Lupu y B. C. Ooi, Peer-to-Peer Computing: Principles and Applications, Springer, 2010.

[12] M. Castro, P. Druschel, A. Ganesh, A. Rowstron y D. S. Wallach, «Secure routing for structured peer-to-peer overlay networks,» *Proceedings of the 5th Usenix Symposium on Operating Systems,* 2002.

[13] G. Urdaneta, G. Pierre y M. V. Steen, «A survey of DHT security techniques,» *ACM Computing Surveys,* 2011.

[14] X. Shen, H. Yu y J. Buford, Handbook of Peer-to-Peer Networking, Springer, 2010.

CAPÍTULO 3

3. EVALUACIÓN DE REDES SOBREPUESTAS PEER-TO-PEER

En este capítulo se evaluan 2 de los principales esquemas para redes sobrepuestas: Chord y CAN. La evaluación de estos sistemas se realiza en base al número de saltos promedio para la realización de una búsqueda, tanto de manera analítica como tambien por medio de resultados de simulacion. Adicionalmente, en este capítulo se evalúa el impacto que tiene la presencia de nodos maliciosos en una red sobrepuesta de tipo Chord, así como su modificiación presente en el protocolo RELOAD. El impacto se mide por medio de un análisis propuesto para obtener la media del número de saltos de una búsqueda exitosa y la probabilidad de búsqueda exitosa. Finalmente, se completa el estudio con la validación del análisis propuesto con resultados de simulación.

3.1 INTRODUCCIÓN

En una red sobrepuesta estructurada, los pares responsables de la información almacenada, así como la ubicación de los mismos dentro del espacio de identificadores, están determinados por la tabla hash distribuida(DHT) sobre la cual está basado el protocolo de la red. Las operaciones principales que la DHT ofrece a la red sobrepuesta son la de inserción y recuperación de un objeto dado una llave. Si un nodo desea insertar información dentro de la red sobrepuesta, primero obtiene la llave correspondiente del objeto a almacenar por medio de la función hash predeterminada. Posteriormente, inicia una búsqueda para determinar el par que se encuentra

más cercano[8] a la llave generada, el cual se le denomina como el par responsable de la llave. La búsqueda puede realizarse en uno o en varios reenvíos (saltos) dependiendo si el par origen cuenta con conexiones directas al par responsable o si se encuentra alejado del mismo en base con la topología de la red sobrepuesta empleada. Una vez localizado el par responsable, se crea una interacción directa entre éste y el par origen para llevar acabo la trasferencia y almacenamiento del objeto. El procedimiento para la recuperación de un objeto almacenado dentro de la red se lleva a cabo de manera similar al de la inserción. Inicialmente se obtiene la llave del objeto que se desea recuperar, para posteriormente realizar la búsqueda del par responsable del mismo y finalmente cuando el nodo responsable ha sido localizado se establece una conexión para el envío de la información deseada.

En la evaluación de una tabla de hash distribuida se consideran diversos aspectos propios de la misma, como lo son: la complejidad de su implementación, la escalabilidad, las medidas de seguridad que proporciona, etc. Sin embargo, como consecuencia de que su objetivo principal es la inserción y el almacenamiento de un objeto determinado, se considera al número de saltos para la realización de una búsqueda dentro de la red como el principal parámetro de evaluación de una DHT.

Por otro lado, dada la flexibilidad que proporcionan actualmente diversas aplicaciones del esquema P2P, se requiere cierto grado de confiabilidad en la recuperación de los objetos en una búsqueda sobre la red sobrepuesta. Por esta razón, otro parámetro que resulta de interés es la probabilidad de búsqueda exitosa, particularmente importante en escenarios donde existen nodos maliciosos perjudicando este procedimiento.

En las siguientes secciones se hace una evaluación de los protocolos Chord [1], CAN [2] y la modificación del protocolo Chord definido en el protocolo RELOAD [3], en base a los parámetros de desempeño: media del número de saltos en una búsqueda exitosa dentro de la red y probabilidad de búsqueda exitosa en presencia de nodos maliciosos.

[8] La distancia y la forma en que se determina ésta, están determinados por la tabla hash distribuida empleada por el protocolo de la red sobrepuesta.

3.2 NÚMERO DE SALTOS PROMEDIO

3.2.1 Chord

El protocolo Chord proporciona las funciones básicas de una tabla hash distribuida de almacenamiento y búsqueda de un par llave-objeto, es decir, dada una llave determinada el protocolo localiza el nodo al cual ésta se mapea. Chord utiliza como base el hash consistente para asignar las llaves a nodos ubicados en una red sobrepuesta de tipo anillo. En Chord el espacio de identificadores está representado por una topología de anillo unidireccional, en la cual los nodos son ubicados de acuerdo su identificador asignado. Cuando una solicitud de búsqueda se genera para un objeto determinado, por medio de la función hash SHA-1 se obtiene la llave correspondiente a ese objeto y se inicia el procedimiento de localización simple o escalable[9] hacia el nodo responsable.

A continuación se realiza un análisis alternativo al presentado en [1] del número de saltos promedio para la realización de una búsqueda en Chord. En este se tienen las siguientes consideraciones:

- El espacio de identificadores de la red es de tamaño 2^m , es decir, se utiliza un tamaño de identificador m.
- Repartidos en el anillo de la red se encuentran N pares.
- Los pares se encuentran uniformemente distribuidos sobre el anillo, a una distancia I :

$$I = \frac{2^m}{N}$$

- Los dedos de cada par están definidos de acuerdo con:

$$dedo_i = sucesor\left(\left(id + 2^{i-1}\right) mod\ 2^m\right) \quad ; \quad 1 \leq i \leq m$$

[9]Una explicación más completa se puede encontrar en el Capítulo 1, sección 1.3.

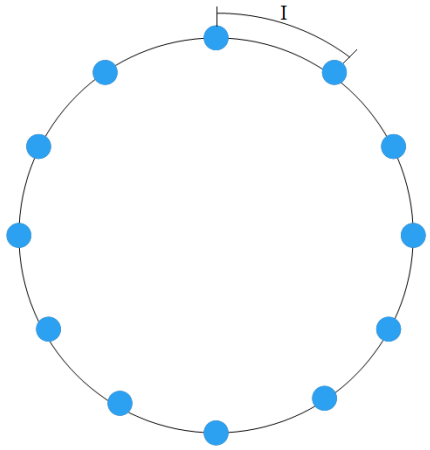


Figura 3.1. Consideraciones del análisis.

El parámetro de desempeño que se desea encontrar es la media de la variable aleatoria número de saltos, desde un nodo origen a un nodo destino cualesquiera dentro de la red sobrepuesta, es decir:

$$\mathbb{E}\{\mathcal{S}\} \quad ; \quad \mathcal{S}\colon v.a.\,número\ de\ saltos$$

El análisis se realiza en base a los saltos que hace un par referentes a la distancia (en número de pares) a la que se encuentra del par destino. Para llevar a cabo los saltos, el nodo cuenta con una tabla de enrutamiento donde están incluidos sus m dedos. A partir de la tabla de enrutamiento, un nodo ocupa aquel dedo que le acerque más al nodo deseado.

A partir de la probabilidad de que se realicen un número de saltos s, dado que se encuentra a una distancia d el par origen del destino:

$$P\{\mathcal{S} = s|\mathcal{D} = d\} \quad ; \quad 0 \leq d \leq N-1$$

Se tiene que, la probabilidad de que se realicen un número de saltos s, está dada por:

$$P\{\mathcal{S} = s\} = P\{\mathcal{S} = s|\mathcal{D} = 0\}P\{\mathcal{D} = 0\} + P\{\mathcal{S} = s|\mathcal{D} = 1\}P\{\mathcal{D} = 1\} + \cdots$$
$$+ \ P\{\mathcal{S} = s|\mathcal{D} = N-1\}P\{\mathcal{D} = N-1\}$$

$$P\{\mathcal{S} = s\} = \sum_{d=0}^{N-1} P\{\mathcal{S} = s|\mathcal{D} = d\}P\{\mathcal{D} = d\}$$

En base a la consideración de que los pares están distribuidos uniformemente:

$$P\{\mathcal{D} = d\} = \frac{1}{N}$$

Entonces:

$$P\{\mathcal{S} = s\} = \frac{1}{N}\sum_{d=0}^{N-1} P\{\mathcal{S} = s|\mathcal{D} = d\}$$

Por lo que la media de los saltos es:

$$\mathbb{E}\{\mathcal{S}\} = \sum_i s_i\, P\{\mathcal{S} = s_i\} = \sum_i s_i \frac{1}{N}\sum_{d=0}^{N-1} P\{\mathcal{S} = s|\mathcal{D} = d\}$$

$$\mathbb{E}\{\mathcal{S}\} = \frac{1}{N}\sum_{d=0}^{N-1}\sum_i s_i P\{\mathcal{S} = s|\mathcal{D} = d\} = \frac{1}{N}\sum_{d=0}^{N-1} \mathbb{E}\{S|\mathcal{D} = d\}$$

Donde el número de saltos que realiza un nodo si se encuentra a una distancia d es:

$$\mathbb{E}\{S|\mathcal{D} = d\} = 1 + \sum_{i=0}^{j_d} \mathbb{E}\{S|\mathcal{D} = d - 2^i\}$$

Con los valores iniciales $\mathbb{E}\{S|\mathcal{D} = 0\} = 0$ y $\mathbb{E}\{S|\mathcal{D} = 1\} = 1$ y j_d como el dedo más cercano al par que se encuentra una distancia d:

$$j_d = max\{j: 2^j \leq d\}$$

Con la función de densidad dada por:

$$f(x) = \sum_i P\{\mathcal{S} = s_i\}\delta(s - s_i)$$

Para la comprobación del modelo analítico se evaluó el protocolo por medio de una simulación, donde se llevaron a cabo múltiples realizaciones de búsquedas en una red estable siguiendo el procedimiento de búsqueda y las consideraciones previamente descritas. En la Figura 3.2 se ilustra la función de densidad de probabilidad para una red de tamaño 2^{12}, con resultados analíticos y simulados. La figura muestra el comportamiento esperado de acuerdo con la Figura 10 de [1], al

presentar resultados muy semejantes a esta. Además se puede observar la media de los saltos con un valor de 6, el cual coincide con $\frac{1}{2}\log_2 N$, donde $N = 4096$.

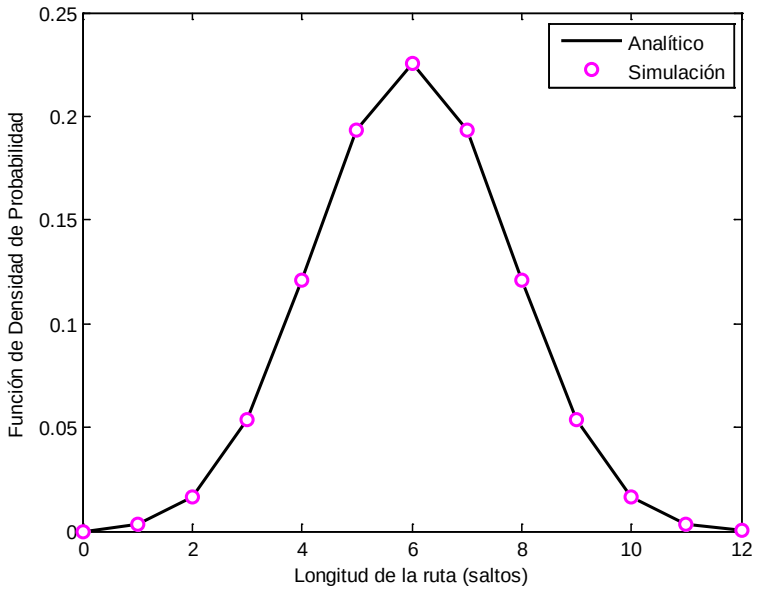


Figura 3.2. Función de densidad de probabilidad de una red de tamaño $N = 4096$, resultados analíticos y resultados simulados.

En la Figura 3.3 se presenta una comparación de la media del número de saltos obtenida por el modelo analítico contra los resultados de la simulación, para diferentes tamaños de red. De la figura se puede observar el comportamiento logarítmico de la media de los saltos descrito en [1], así como la validación de la expresión analítica demostrada previamente.

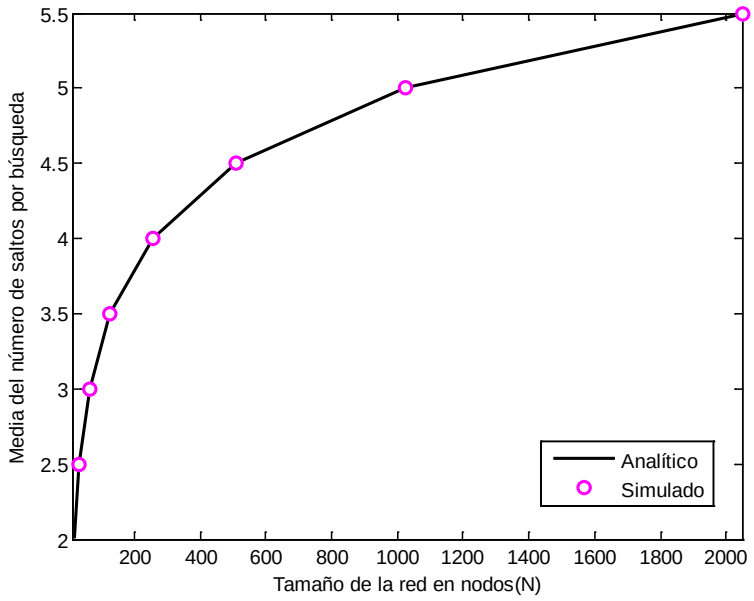


Figura 3.3. Comparación de los resultados analíticos contra los resultados obtenidos de la simulación, cuando $N = 2^i \;\; i = 4, \ldots, 11$.

3.2.2 CAN

El sistema distribuido CAN proporciona las funcionalidades de una tabla hash distribuida de inserción y almacenamiento de objetos en la red dada su correspondiente llave, brindando además escalabilidad y robustez contra fallas. En CAN los nodos y los objetos son ubicados en base al mapeo de las llaves a un punto en el espacio coordenado d-dimensional. El procedimiento de localización de un objeto dentro del sistema se realiza por medio de solicitudes de búsqueda a aquel nodo perteneciente a la tabla de vecinos del par que se encuentre a la menor distancia euclidiana del destino [4].

Para el análisis del número de saltos promedio presentado, se utilizan las siguientes consideraciones:

- El espacio d-dimensional se reparte entre los nodos de manera equitativa, es decir, se parte en n zonas del mismo tamaño, donde n es el número de nodos presentes en la red.
- Los nodos en el sistema tienen dos vecinos por cada dimensión del espacio coordenado, en otros términos, la tabla de vecinos de un nodo es de $2d$.

- El espacio coordenado es un espacio d-toroidal.

El parámetro de desempeño que se desea encontrar es la media de la variable aleatoria número de saltos, desde un nodo origen a un nodo destino cualesquiera dentro del espacio coordenado, es decir:

$$\mathbb{E}\{\mathcal{S}\} \quad ; \quad \mathcal{S}\colon\ v.a.\text{número de saltos}$$

El análisis se realiza en base a los saltos que hace un par referentes a la distancia cartesiana a la que se encuentra del par destino.

$$\mathbb{E}\{\mathcal{D}\} \quad ; \quad D\colon\ v.a.\text{distancia cartesiana}$$

La media de la distancia cartesiana está dada por:

$$\mathbb{E}\{\mathcal{D}\} = \frac{d_{max} - d_{min}}{2}$$

Sin embargo, debido a que el avance dentro del espacio coordenado se realiza de manera discreta por el cruce de peticiones de búsqueda por las zonas de los nodos vecinos, la distancia cartesiana puede medirse en términos de las zonas que se atraviesan para llegar al destino (número de saltos); por lo que para un toroide d-dimensional:

$$d_{max} = \sum_{i=1}^{d} \frac{\sqrt[d]{n}}{2} \qquad y \qquad d_{min} = 0$$

Con lo cual se obtiene:

$$\mathbb{E}\{\mathcal{D}\} = \frac{d}{4}\sqrt[d]{n} = \mathbb{E}\{\mathcal{S}\}$$

Para la comprobación del modelo analítico se evaluó el protocolo por medio de una simulación, donde se llevaron a cabo múltiples realizaciones de búsquedas en una red estable siguiendo el procedimiento de búsqueda y las consideraciones previamente descritas, evaluando para diferentes tamaños de red y diferentes dimensiones. En la Figura 3.4 se presenta una comparación de los datos obtenidos por el modelo analítico contra los resultados de la simulación.

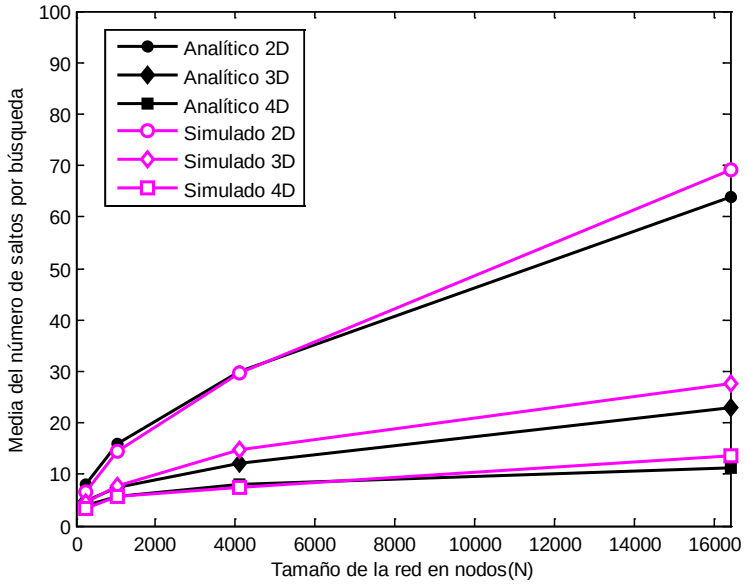


Figura 3.4. Comparación modelo analítico contra el modelo simulado de CAN, para diferentes tamaños de red.

La discrepancia en la Figura 4, entre los datos simulados y los datos del modelo analítico, se debe a que el modelo analítico se basa en la suposición de que la repartición de las zonas se hace de manera uniforme. Sin embargo, en el sistema no se presenta esta uniformidad, ya que existen pares con zonas de responsabilidad mayores a las de sus vecinos o a las de otros pares en el sistema. En [4] se propone una modificación al esquema de repartición para mejorar la uniformidad en CAN. Esta modificación consiste en verificar las zonas adyacentes de un nodo y asignar el par llave-objeto a aquel nodo cuya zona sea menor al momento de la asignación de responsabilidades. Sin embargo, en el estudio realizado se utiliza el sistema básico de CAN, es decir no se implementaron todas las propuestas de mejoría para la simulación de la red. A pesar de que los datos no tienen coincidencia, de la figura se aprecia que tienen un comportamiento $\mathcal{O}\left(N^{1/d}\right)$ semejante, lo que permite validar el simulador tomando en consideración lo antes mencionado.

3.2.3 Comparativa Chord contra CAN

En la actualidad son diversas las comparativas que se han realizado entre los diferentes esquemas de las redes sobrepuestas P2P. Con la aparición de los sistemas DHT referencia, como lo son: Chord, CAN, Pastry y Kademlia; se realizaron evaluaciones referentes a sus características de construcción. En [5] se hace una comparativa referente a los procedimientos de selección de los pares adyacentes, los mecanismos de almacenamiento y su redundancia, la búsqueda e inserción de los objetos en la red, la permanencia de los datos en el sistema, así como las propiedades de tolerancia contra fallas. Así mismo, en [6] se hace una clasificación de los trabajos realizados en dirección a las redes *Peer-to-Peer* en las categorías de procedimientos de búsqueda, procesos de almacenamiento, la seguridad proporcionada por los esquemas analizados, así como sus implementaciones y aplicaciones hasta la fecha de su publicación. Posteriormente, en los años subsecuentes, se realizaron estudios sobre comportamientos y escenarios particulares. En [7] se realiza una observación relativa al costo en términos del tráfico generado que introduce la topología empleada, así como al tamaño de la información de enrutamiento y sus períodos de actualización ante períodos de entrada y salida continuos de los pares. Un estudio sobre la similitud de la red subyacente y la red sobrepuesta empleada, comparando la media de saltos contra la latencia de una búsqueda en diversos esquemas de redes sobrepuestas con múltiples nodos fallidos, se presenta en [8]. Recientemente, los estudios comparativos entre los diversos esquemas DHT se centran en la evaluación de los mismos sobre redes inalámbricas [9], en plataformas de simulación específicas [10] o para evaluar el impacto que tienen ataques de seguridad específicos en diferentes esquemas de red sobrepuesta, como en [11]. En la Tabla 1, se ilustran de manera breve las diferencias entre los dos esquemas analizados.

Característica	CAN	Chord
Arquitectura de la DHT	Espacio coordenado de identificadores multidimensional	Espacio de identificadores unidireccional y circular.
Asignación par (objeto,identificador)	Al aplicar la función hash al identificador o llave se obtiene un punto en el espacio.	Al aplicar la función hash al objeto se obtiene su identificador.
Parámetros del sistema	N: Número de pares en el sistema. d: Número de dimensiones	N: Número de pares en el sistema.
Procedimiento de búsqueda	El nodo origen dirige la búsqueda a aquel nodo cuyas coordenadas cartesianas estén más cerca del destino.	El nodo origen dirige la búsqueda a aquel nodo que se aproxime más al destino en el anillo.
Número de saltos promedio por búsqueda	$\mathcal{O}\left(d\sqrt[d]{N}\right)$	$\mathcal{O}(\log N)$
Tamaño de la tabla de enrutamiento	$2d$	$\log N$
Independencia en el enrutamiento	Presenta múltiples rutas independientes.	Presenta una ruta independiente.
Tolerancia a fallas	La presencia de nodos fallidos afecta de manera local. Puede implementarse replicación en los vecinos.	La presencia de nodos fallidos afecta de manera local. Puede implementarse replicación en los sucesores.

Tabla 1. Comparativa entre los esquemas de redes sobrepuestas P2P, Chord y CAN.

A continuación se muestra una comparación cuantitativa de la media de saltos promedio bajo los esquemas Chord y CAN, para diferentes tamaños de red y variando las dimensiones en CAN. En la Figura 3.5 se observa la semejanza de comportamiento que presentan los dos sistemas, puesto que los sistemas mantienen una relación logarítmica con el número de nodos presentes en la red. Adicionalmente se puede ver que la red de nodos que utilizan Chord como protocolo de red sobrepuesta tiene un mejor desempeño contra una red que utiliza CAN de 2 y 3 dimensiones, el cambio ocurre cuando el espacio coordenado es de 10 dimensiones, en cuyo caso el desempeño del sistema es ligeramente mejor que el de Chord.

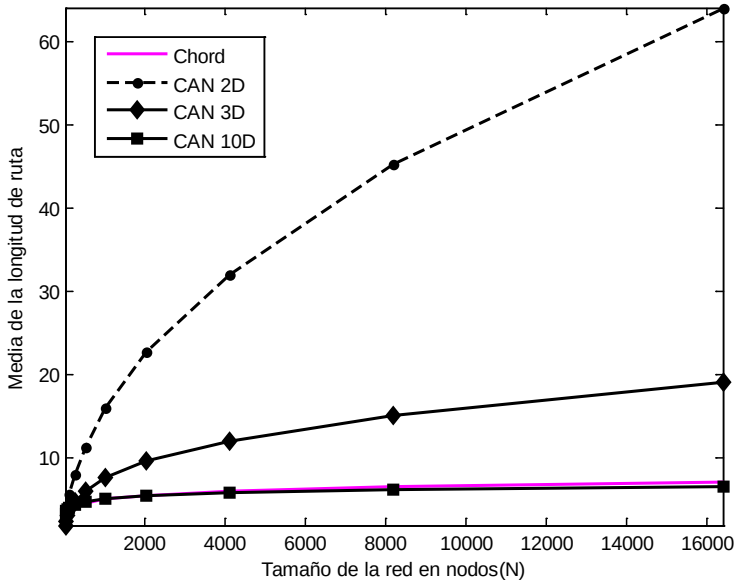


Figura 3.5. Comparativa de la media del número de saltos en el procedimiento de búsqueda para Chord y CAN de 2,3 y 10 dimensiones.

A pesar de que ambos esquemas presentan características deseables y no deseables, la elección de uno particular está completamente ligada a los servicios y aplicaciones que se quieran ofrecer dentro de la red *Peer-to-Peer*. Sin embargo se ha elegido al protocolo Chord como objeto de estudio en lo sucesivo, debido a lo siguiente:

- Chord presenta una geometría unidimensional, lo que se traduce en una arquitectura simple y con un nivel de implementación menor al de CAN.
- Una mejora de desempeño en CAN se puede realizar modificando parámetros como lo son el número de dimensiones o el número de realidades. Sin embargo, estos parámetros no permiten que el sistema escale de manera dinámica puesto que son determinados previos a la construcción de una red. Esta característica impide la utilización de una sola configuración eficiente para ambientes con poblaciones de alta variación. Así mismo, un aumento de estos parámetros de mejora involucra un aumento en el costo y la complejidad del sistema.
- Como se puede apreciar en la Figura 3.5, el desempeño de CAN con respecto al de Chord en relación al número de saltos realizados en una búsqueda para una red de N pares, sólo es superior cuando se manejan dimensiones mayores a $d = \frac{1}{2}\log_2 N$. Un sistema con

dicha construcción requiere de mayor capacidad de procesamiento, así como de tiempo de ejecución, para su simulación, que su equivalente en desempeño de Chord.

3.2.4 Chord-RELOAD

El RFC 6940 establece como protocolo preestablecido para la topología de la red sobrepuesta una modificación del protocolo Chord. Esta modificación presenta entre otras, el uso de una lista de sucesores y predecesores de tamaño 3 con el fin de combatir las fallas de los nodos en la red. Adicionalmente, la lista de sucesores dentro de la tabla de enrutamiento de un nodo altera el desempeño de la red con respecto al número de saltos promedio. Enseguida se presenta un análisis similar al de la sección 3.2.1 que incluye el efecto de la adición de sucesores en la tabla de enrutamiento.

Tomando en cuenta las mismas consideraciones presentadas en la sección 3.2.1, a partir de la probabilidad de que se realicen un número de saltos s, dado que se encuentra a una distancia d el par origen del destino:

$$P\{\mathcal{S} = s|\mathcal{D} = d\} \quad ; \quad 0 \leq d \leq N-1$$

Se tiene que, la probabilidad de que se realicen un número de saltos s, está dada por:

$$P\{\mathcal{S} = s\} = \sum_{d=0}^{N-1} P\{\mathcal{S} = s|\mathcal{D} = d\}P\{\mathcal{D} = d\}$$

En base a la consideración de que los pares están distribuidos uniformemente, se obtiene:

$$P\{\mathcal{S} = s\} = \frac{1}{N}\sum_{d=0}^{N-1} P\{\mathcal{S} = s|\mathcal{D} = d\}$$

Por lo que la media de los saltos es:

$$\mathbb{E}\{\mathcal{S}\} = \frac{1}{N}\sum_{d=0}^{N-1}\sum_{i} s_i P\{\mathcal{S} = s|\mathcal{D} = d\} = \frac{1}{N}\sum_{d=0}^{N-1}\mathbb{E}\{S|\mathcal{D} = d\}$$

Donde el número de saltos que realiza un nodo si se encuentra a una distancia d es:

$$\mathbb{E}\{S|\mathcal{D}=d\} = 1 + \sum_{i=0}^{j_d} \mathbb{E}\{S|\mathcal{D}=d-2^i\}$$

Puesto que se considera una lista de sucesores de tamaño r=3, ahora los valores iniciales son:

$$\mathbb{E}\{S|\mathcal{D}=i\} = \begin{cases} 0 & i=0 \\ 1 & i=1,2,3 \end{cases}$$

Con j_d como el dedo más cercano al par que se encuentra una distancia d:

$$j_d = max\{j: 2^j \leq d\}$$

Para la comprobación del modelo analítico se evaluó el protocolo por medio de una simulación, donde se llevaron a cabo múltiples realizaciones de búsquedas en una red estable siguiendo el procedimiento de búsqueda y las consideraciones previamente descritas, evaluando para diferentes tamaños de red. En la Figura 3.6 se presenta una comparación de los datos obtenidos por el modelo analítico contra los resultados de la simulación. La figura muestra la validez del modelo analítico para la obtención de la media de saltos en Chord, al tener valores de simulación coincidentes con los esperados del modelo.

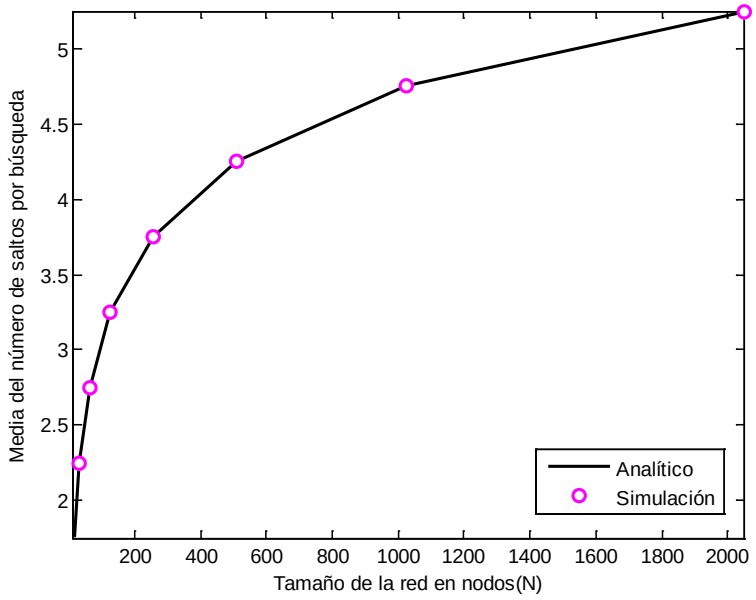


Figura 3.6. Validación del modelo analítico para la obtención de la media del número de saltos por búsqueda, a través de los resultados obtenidos por simulación.

3.3 EVALUACIÓN EN LA PRESENCIA DE NODOS MALICIOSOS.

3.3.1 Introducción

Las redes *Peer-to-Peer* basadas en tablas de hash distribuidas además de presentar los ataques inherentes a las redes distribuidas como los son la negación de servicio o la implantación y distribución de archivos malintencionados, sufren de ataques referentes a las operaciones básicas de inserción y recuperación de objetos. Estos ataques son realizados en mayor parte por la presencia de nodos maliciosos, ya sea por medio de la creación de identidades Sybil o por la existencia de usuarios malintencionados, al igual que por la corrupción de nodos honestos. [12] Una vez que los nodos maliciosos se encuentran posicionados en la red, estos pueden manipular las peticiones de búsqueda, las tablas de enrutamiento o redirigir los mensajes y retener los objetos. En la Tabla 2 se muestran de manera sintetizada los ataques a los procedimientos de inserción y recuperación de objetos que se pueden realizar en una DHT de tipo Chord, así como algunas soluciones introducidas hasta la actualidad.[10]

		Defensas					
		Restricción de las entradas en las tablas de ruteo	Uso de tablas de ruteo redundantes	Auditoría interna	Uso de mecanismos de replicación	Empleo de certificados de responsabilidad	Actualización periódica de las tablas de ruteo
Ataques	Manejo malicioso de los recursos almacenados				●	●	
	Enrutamiento malicioso	●	●	●	●		
	Alteración de las tablas de ruteo en la actualización de la red	●	●	●			●
	Man in the middle routing attack	●	●	●	●		

Tabla 2. Ataques en los procedimientos de inserción y recuperación de un objeto en Chord.

[10] Para una explicación más detallada de los ataques en las redes P2P, así como a sus posibles soluciones, referirse al Capítulo 2.

En esta sección se evalúan las consecuencias de la presencia de nodos maliciosos sobre el desempeño de una red P2P bajo el esquema Chord referentes a la media de la longitud de la búsqueda y a la probabilidad de búsqueda exitosa.

3.3.2 Modelo de adversarios

El principal objetivo de un ataque a los procedimientos de inserción y recuperación de un objeto o, como también pueden ser referidos, de almacenamiento y enrutamiento, es evitar que la búsqueda de un objeto sea exitosa, es decir, que el objeto no pueda obtenerse. Sin embargo, el comportamiento que presente un nodo malicioso con este fin puede ser muy diverso. Por ejemplo, un atacante puede rehusarse a dirigir la búsqueda hacia el siguiente salto, o podría dirigirla hacia un nodo incorrecto, no existente, o a uno malicioso. Así mismo, el atacante puede dirigir las búsquedas de manera correcta, pero cuando recibe una petición de búsqueda hacia un objeto del cual es responsable, niega su existencia.

De manera particular, los nodos maliciosos considerados en este estudio presentan las siguientes características:

- El nodo no dirige ninguna petición de búsqueda, sin restricción alguna.
- No existen nodos en coalición, es decir, todos los nodos maliciosos actúan de manera independiente entre sí.
- Un nodo malicioso no puede elegir su ubicación en el anillo, puesto que su identificador es asignado de acuerdo con el protocolo y sólo le es asignado una vez.
- Cuando el nodo malicioso es responsable de un objeto o es el último salto, no es posible la recuperación del objeto.

3.3.3 Evaluación sobre Chord

Desde la aparición de Chord se han realizado diversos estudios con el fin de disminuir el efecto que tienen los nodos maliciosos en la longitud promedio de la búsqueda y en la probabilidad de búsqueda exitosa. En [13] se discute la relación que presenta la existencia de múltiples trayectorias independientes con la robustez del sistema contra nodos adversos. Sin embargo, una trayectoria

independiente requiere que en una ruta de n saltos, $n-1$ nodos intermedios no coincidan con otra trayectoria semejante, desde el mismo nodo origen al mismo nodo destino, lo cual es difícilmente alcanzable en muchos de los esquemas de redes sobrepuestas.[11] En [14] se hace una evaluación por medio de simulación de los efectos de una red Chord bajo la presencia de nodos maliciosos y se concluye que una de las principales razones por las que es susceptible a sus ataques es su arquitectura unidireccional. A pesar de que los estudios realizados proporcionan una mirada a las consecuencias de contar con nodos adversos en la red sobrepuesta, la gran mayoría de los resultados y propuestas de solución están basados en resultados por simulación. Por consiguiente, en esta sección se realiza un análisis probabilístico que refleje los cambios en una red infectada por nodos malintencionados, en términos de los parámetros de desempeño: longitud promedio de la ruta y probabilidad de búsqueda exitosa.

El análisis es similar al realizado en la sección 3.2.1 y se tienen las siguientes consideraciones:

- El espacio de identificadores de la red es de tamaño 2^m , es decir, se utiliza un tamaño de identificador m.
- Repartidos en el anillo de la red se encuentran N pares.
- Los pares se encuentran uniformemente distribuidos sobre el anillo, distanciados entre ellos a una unidad.
- Los dedos de cada par están definidos de acuerdo con:

$$dedo_i = sucesor\left(\left(id + 2^{i-1}\right) mod\ 2^m\right) \quad ; \quad 1 \leq i \leq m$$

- La probabilidad de que un nodo sea malicioso es f.
- La probabilidad de que un nodo sea malicioso es independiente de que otro nodo sea malicioso.

El parámetro de desempeño que se desea encontrar es la media de la variable aleatoria *número de saltos* en una búsqueda exitosa, desde un nodo origen a un nodo destino cualesquiera dentro de la red sobrepuesta, cuando existe una fracción f de nodos maliciosos en el anillo, es decir:

$$\mathbb{E}\{\mathcal{S}\} \quad ; \quad \mathcal{S}\colon\ v.a.\ número\ de\ saltos$$

[11] Cabe resaltar que en Chord sólo existe una trayectoria independiente para cualquier búsqueda en el anillo.

El análisis se realiza basado en los saltos a los cuales un par origen se encuentra del par destino y a la distancia (en número de pares) a la que están dentro del anillo. Para llevar a cabo los saltos, el nodo cuenta con una tabla de enrutamiento donde están incluidos sus m dedos. A partir de la tabla de enrutamiento, un nodo ocupa aquel dedo que le acerque más al nodo deseado, siempre que esta opción sea confiable.

Con la probabilidad de que se realicen un número de saltos s, dado que se encuentra a una distancia d el par origen del destino:

$$P\{\mathcal{S} = s|\mathcal{D} = d\} \quad ; \quad 0 \leq d \leq N-1$$

Se tiene que, la probabilidad de que se realicen un número de saltos s, está dada por:

$$P\{\mathcal{S} = s\} = \sum_{d=0}^{N-1} P\{\mathcal{S} = s|\mathcal{D} = d\}P\{\mathcal{D} = d\}$$

En base a la consideración de que los pares están distribuidos uniformemente:

$$P\{\mathcal{D} = d\} = \frac{1}{N}$$

Entonces:

$$P\{\mathcal{S} = s\} = \frac{1}{N}\sum_{d=0}^{N-1} P\{\mathcal{S} = s|\mathcal{D} = d\}$$

Por lo que la media de los saltos es:

$$\mathbb{E}\{\mathcal{S}\} = \frac{1}{N}\sum_{d=0}^{N-1}\sum_{i} s_i P\{\mathcal{S} = s|\mathcal{D} = d\} = \frac{1}{N}\sum_{d=0}^{N-1}\mathbb{E}\{\mathcal{S}|\mathcal{D} = d\}$$

Nombrando, la media de saltos para una búsqueda exitosa dado que se encuentra a una distancia d, como:

$$\mathbb{E}\{\mathcal{S}|\mathcal{D} = d\} = s(d) \qquad d = 0,1,\dots,N-1$$

Donde, debido a la construcción y las consideraciones del sistema, se tienen las siguientes condiciones iniciales:

$$s(d) = \begin{cases} 0 & d = 0 \\ 1 & d = 2^i \ ; i = 0, .., m-1 \end{cases}$$

Para la evaluación de la media del número de saltos condicional no es posible derivar una expresión cerrada como en la sección 3.2.1, esto debido a lo siguiente:

- La expresión presentada en la sección 3.2.1 es un caso particular en el cual todas las trayectorias de búsqueda dentro de la red son exitosas, es decir, la probabilidad de búsqueda fallida es cero. En el escenario actual, la presencia de nodos maliciosos conlleva a que existan trayectorias cuya búsqueda resulte inconclusa. Además, puesto que para dirigir una búsqueda se elige aquel nodo confiable dentro de la tabla de enrutamiento que se acerque más al destino, las trayectorias resultantes se extienden en cuanto al número de saltos con el fin de evitar nodos adversos.
- Una expresión recursiva para el cálculo de las media de los saltos condicionados basada en los grafos probabilísticos de Lee [15] podría parecer adecuada, sin embargo el sistema presenta características de un modelo no independiente. En la figura 3.7 se muestra un ejemplo de análisis con el uso de un grafo probabilístico, para cuando $d = 5$.

  En la figura se muestran todas las posibles trayectorias que realiza una petición de búsqueda desde un nodo origen a un nodo destino, cuando estos están a una distancia de 5 nodos. En las ramas del grafo se ilustran las probabilidades de ser utilizadas, dependiendo si el dedo más cercano es malicioso o no. Al final de cada rama, se coloca el número de saltos que conlleva seguir esta rama particular, así como la probabilidad de hacerlo. Nótese que la probabilidad en cada rama aún no está condicionada a que sea una búsqueda exitosa, la condicional se realiza posteriormente al evaluar todas las trayectorias probables que alcanzan el destino. De la figura también se puede observar el procedimiento recursivo implicado, donde las distancias menores a 5 pueden resolverse a partir de los grafos previamente calculados $s(4)$ y $s(3)$.

  Sin embargo, dado que el dedo i de un nodo a puede ser el nodo j de un nodo b, para $i, j = 1, \dots, m-1$, lo que implica que los dos nodos que tienen cada uno de los pares en su tabla de enrutamiento pueden ser el mismo nodo malicioso. Esta particularidad tiene como consecuencia que las ramas en el grafo no sean independientes.

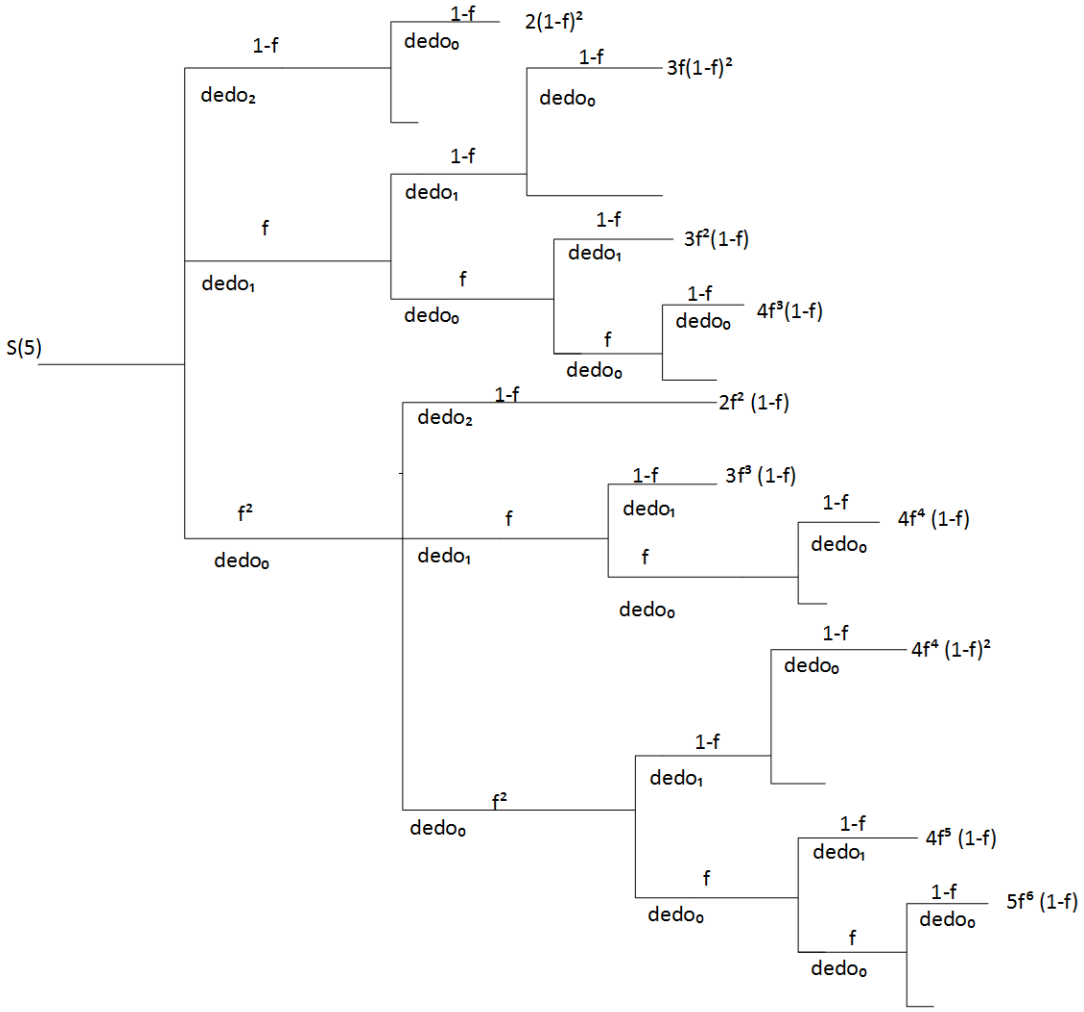


Figura 3.7. Grafo probabilístico para el cálculo de la media de saltos de una búsqueda exitosa, dado que se está a una distancia $d = 5$.

Para la evaluación de la media de saltos para una búsqueda exitosa dado que se encuentra a una distancia d, se ocupó el siguiente algoritmo. El algoritmo permite obtener las ramas de un grafo probabilístico de trayectorias incluyendo las particularidades antes mencionadas.

```
ALGORITMO: busqueda
INPUT: nodOri, nodDes, nodosMal, saltos
OUTPUT: longitud, saltos
no2Mal ← NodosMal
saltos ← saltos + 1
for i=m:0
    nodo ← 2^i + nodOri
    if nodo < nodDes & nodo ∉ nod2Mal
        if busqueda(nodo,nodDes,no2Mal,saltos) ==
1
            saltos ← saltos + 1
        end if
        no2Mal ← agrega(nodo)
    end if
    else if nodo == nodDes
        saltos ← saltos + 1
        longitud ← tamaño(no2Mal)
        return saltos,longitud
    end if
end for
return -1
```

El algoritmo funciona de la siguiente manera:

- El cálculo de las medias de saltos para cada uno de los valores de d se realiza invocando recursivamente el algoritmo de búsqueda con los parámetros de entrada dados por:

  `nodOri = dedoMayorNoMalicioso()`

  `nodoDestino = d`

  `nodosMal = {}`

  `saltos = 0`

  El `dedoMayorNoMalicioso()` es aquel nodo potencia de 2 que está más cercano al destino pero que no forma parte del conjunto de nodos maliciosos. Una vez que el algoritmo ha regresado de la recursión, el `dedoMayorNoMalicioso` se agrega al conjunto de nodos maliciosos `nodMal` y se repite el proceso hasta que se acaben los nodos potencias de dos posibles.

- El algoritmo de búsqueda recorre de manera recursiva todas las posibles trayectorias, bajo el mismo principio de búsqueda que utiliza Chord. Se escoge al nodo que posee un identificador menor al identificador del nodo destino pero que también disminuya la distancia nodo origen-destino máxima, siempre que el nodo no se encuentre en el conjunto de nodos maliciosos. En el caso de que el nodo que represente la mejor opción sea parte del conjunto de nodos adversos, se escoge la segunda mejor opción, y así sucesivamente hasta que las trayectorias posibles se agoten.
- El algoritmo de búsqueda tiene como salida el número de saltos que se realizaron al recorrer una determinada trayectoria, así como la cantidad de nodos maliciosos que se encontraron en la misma. Estos parámetros de salida deben ser almacenados para la futura ponderación de las ramas, con la cual se condiciona a una búsqueda de carácter exitoso. Entonces, la media del número de saltos dada una distancia d para una búsqueda exitosa, es:

$$s(d) = \frac{\sum_i saltos_i f^{longitud_i}(1-f)^{saltos_i+1}}{\sum_i f^{longitud_i}(1-f)^{saltos_i+1}}$$

Donde:

i	$i = 1, \ldots, n\acute{u}meroDeTrayectorias(d)$
$n\acute{u}meroDeTrayectorias(d)$	Número de trayectorias de la distancia d
$saltos_i$	Número de saltos en la trayectoria i
$longitud_i$	Número de nodos maliciosos en la trayectoria i

La comprobación del modelo analítico y del algoritmo de trayectorias se realizó por medio de una simulación, donde se llevaron a cabo múltiples realizaciones de búsquedas en una red estable siguiendo el procedimiento de búsqueda y las consideraciones previamente descritas, evaluando para diferentes tamaños de red. En la Figura 3.8 se presenta una comparación de los datos obtenidos por el modelo analítico contra los resultados de la simulación, en términos de la media del número de saltos. Asimismo, se observa la validez de los resultados obtenidos por medio del

modelo analítico propuesto al ajustarse a los obtenidos en la simulación, aún bajo la presencia de porcentajes de nodos maliciosos diferentes.

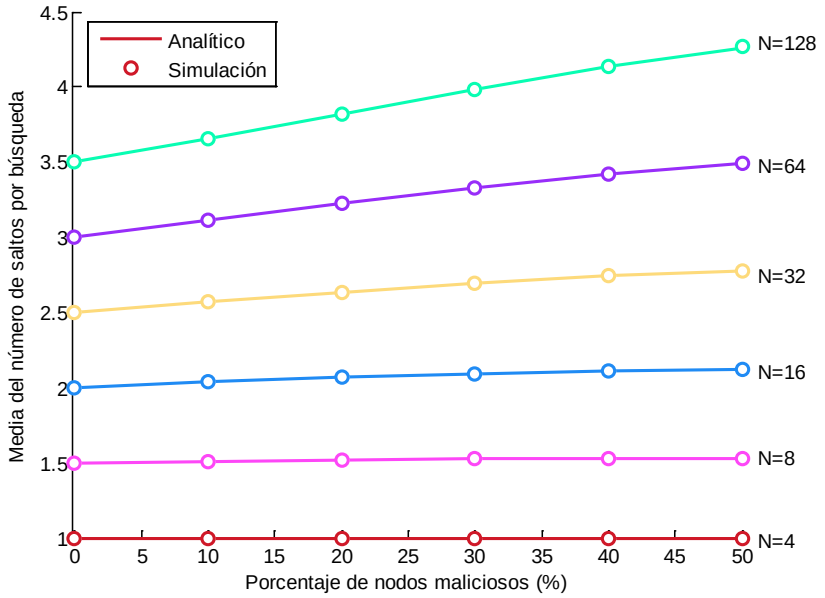


Figura 3.8. Validación del modelo analítico a través de simulación.

El segundo parámetro de desempeño estudiado es la probabilidad de búsqueda exitosa, la cual se puede obtener de manera directa del algoritmo generador de trayectorias, a partir de la expresión:

$$Probilidad\ búsqueda\ exitosa = \sum_{d=0}^{N-1} \sum_{i_d} f^{longitud_{i_d}} (1-f)^{saltos_{i_d}+1}$$

Donde:

i_d	$i_d = 1, \ldots., número De Trayectorias(d)$
$número De Trayectorias(d)$	Número de trayectorias de la distancia d
$longitud_{i_d}$	Número de nodos maliciosos en la trayectoria i_d

En la Figura 3.9 se muestra la probabilidad de búsqueda exitosa derivada del modelo analítico y la derivada de la simulación. En esta se varían el tamaño de la red y el porcentaje de nodos maliciosos presentes en la misma.

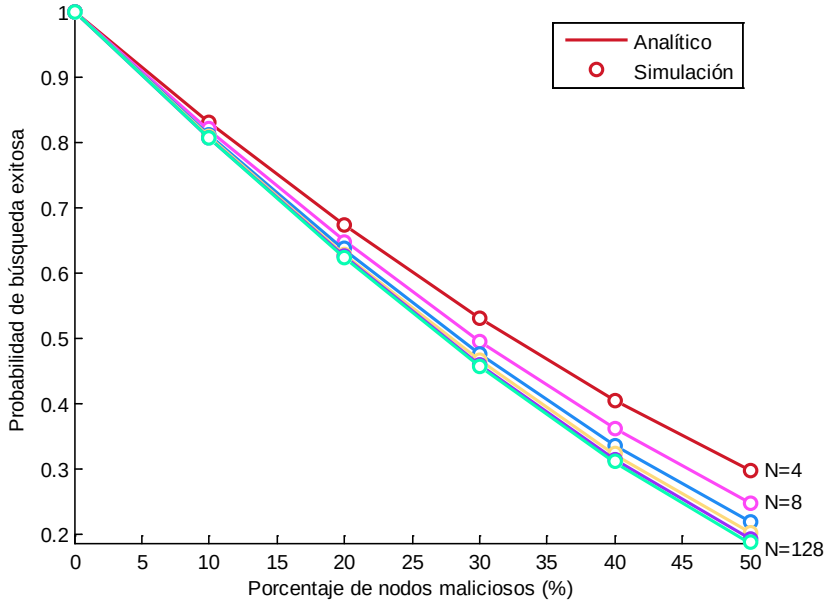


Figura 3.9. Probabilidad de búsqueda exitosa, resultados del modelo analítico y de la red simulada.

La Figura 3.9 muestra la verdadera amenaza que representan los nodos maliciosos en la red, ya que a pesar de que la métrica de la media del número de saltos no se ve afectada en gran medida cuando se tiene una búsqueda exitosa, el porcentaje de que una búsqueda se complete resulta seriamente afectado por los nodos que malintencionadamente alteran los procedimientos de búsqueda. Por ejemplo, de manera numérica, para un porcentaje de nodos maliciosos del 20% en una red de 128 nodos, la media del número de saltos sufre un incremento de aproximadamente 10% cuando la búsqueda se puede realizar. Sin embargo, de todas las búsquedas intentadas sólo el 62.4% se pueden completar de manera exitosa.

Comparativa del modelo propuesto con análisis presentados en la literatura

Para mostrar la validez de la solución analítica propuesta en este trabajo, a continuación se comparan los resultados que se desprenden de algunas evaluaciones encontradas en la literatura. Los resultados que aquí se presentan son de aquellas referencias que han tenido mayor impacto, en concreto se muestran los resultados presentados en [1] y en [13]. Cabe señalar que el trabajo sobre Chord, [1], no presenta un análisis para evaluar la seguridad de la red en presencia de nodos maliciosos, sino que presenta una expresión para la media del número de saltos cuando se presentan fallas en la red. Sin embargo, bajo el modelo de adversarios presentado en esta sección, un nodo malicioso podría confundirse con un nodo fallido, con la excepción de que un nodo fallido eventualmente podría ser eliminado de las posibles rutas después de las etapas de mantenimiento de la red; mientras que un nodo malicioso seguirá formando parte de las rutas, aún después del proceso de actualización y mantenimiento. Otra particularidad que exhibe la expresión en [1] es que presenta errores numéricos, posiblemente en la escritura de la expresión, por lo que la expresión que se utilizó para la comparación en esta sección es la siguiente:

$$\mathbb{E}\{\mathcal{S}\} = \frac{1}{2}\log_d N$$

Donde:

$$d = \frac{1}{2}\left[\frac{1-f}{1-f/2}\right]^{-1}$$

La expresión anterior resulta de buscar la corrección de la expresión ilustrada en [1], siguiendo la metodología presentada en el mismo.

En cuanto a los resultados presentados en [13], éstos se derivan del análisis realizado bajo la suposición de que una búsqueda incorrecta puede ser detectada, es decir, se verifica que con cada salto en la búsqueda, la petición se acerque al nodo destino. La media del número de saltos en una búsqueda se presenta como:

$$\mathbb{E}\{\mathcal{S}\} = \frac{\frac{1}{2}\log_2 N}{1-f}$$

En la Figura 3.10 se muestran los resultados del Análisis 1 presentado en [1], del Análisis 2 presentado en [13] y el propuesto en la sección 3.3.3 (Análisis 3), junto con los resultados de la simulación.

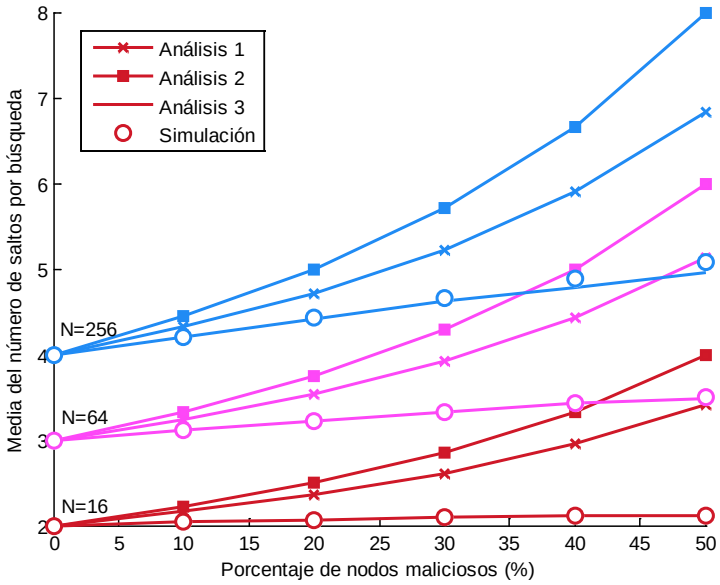


Figura 3.10. Comparativa de la media del número de saltos por búsqueda entre el análisis 1 [1], el análisis 2 [13], el análisis propuesto y los resultados de la simulación.

En la Figura 3.10 se observa que tanto el Análisis 1, como el Análisis 2 no reflejan la situación actual del sistema, puesto que los dos modelos se alejan de los datos arrojados por la simulación. Esta tendencia se debe a que ninguno de los dos análisis toma en cuenta la existencia de un nodo malicioso en las tablas de enrutamiento de diferentes nodos, por lo que un mismo nodo malicioso puede aparecer en diferentes trayectorias de búsqueda para diferentes nodos origen. Los análisis realizados no toman en cuenta la consideración anterior, sino que sólo se refieren a la proporción de distancia en el anillo que se va disminuyendo a cada salto, conforme aumenta el porcentaje de nodos maliciosos existentes en la red.

3.3.4 Evaluación sobre Chord-RELOAD

La modificación de Chord realizada en el protocolo RELOAD presenta el uso de una lista de sucesores y predecesores de tamaño 3 con el fin de combatir las fallas de los nodos en la red. El análisis referente a la variación de los parámetros de desempeño estudiados que se deriva de la modificación de Chord en RELOAD, se presenta a continuación.

Bajo las mismas consideraciones de la sección 3.3.3, la probabilidad de que se realicen un número de saltos s, dado que se encuentra a una distancia d el par origen del destino:

$$P\{\mathcal{S} = s|\mathcal{D} = d\} \quad ; \quad 0 \leq d \leq N-1$$

Se tiene que, la probabilidad de que se realicen un número de saltos s, está dada por:

$$P\{\mathcal{S} = s\} = \frac{1}{N}\sum_{d=0}^{N-1} P\{\mathcal{S} = s|\mathcal{D} = d\}$$

Por lo que la media de los saltos es:

$$\mathbb{E}\{\mathcal{S}\} = \frac{1}{N}\sum_{d=0}^{N-1} \mathbb{E}\{S|\mathcal{D} = d\}$$

Nombrando, la media de saltos para una búsqueda exitosa dado que se encuentra a una distancia d, como:

$$\mathbb{E}\{S|\mathcal{D} = d\} = s(d) \qquad d = 0,1,\dots,N-1$$

Donde, con el aumento de $r = 3$ sucesores en la tabla de enrutamiento, se tienen las siguientes condiciones iniciales:

$$s(d) = \begin{cases} 0 & d = 0 \\ 1 & d = 2^i \ ; i = 0,..,m-1 \quad \text{ó} \quad d = 1,2,3 \end{cases}$$

El cálculo de la media del número de saltos para una búsqueda exitosa dada una distancia d se puede evaluar utilizando el algoritmo presentado en la sección 3.3.3. En la Figura 3.11 se muestra la comprobación del método analítico contra la simulación de un sistema estable, con variaciones en el porcentaje de nodos maliciosos presentes en el sistema y en el tamaño de la red. En la figura

se observa la similitud entre los datos obtenidos por medio del modelo analítico contra los resultados de la simulación, sin embargo, para $N = 256$ con 50% de nodos maliciosos el resultado del modelo analítico se encuentra por debajo del resultado simulado. Esto se debe a que conforme al tamaño de la red incrementa y el porcentaje de nodos maliciosos aumenta, el número de trayectorias posibles también presenta un aumento. Durante la evaluación del algoritmo de trayectorias, el número de trayectorias determina el costo del procesamiento, así como el tiempo de ejecución, por lo que, si la cantidad de rutas alternativas aumenta también lo hará su procesamiento. Para disminuir el costo de procesamiento del algoritmo, se descartan aquellas trayectorias cuya aportación al promedio es del orden de 0.0009. A pesar de que se tiene una gran cantidad de trayectorias que se encuentran dentro de este rango, la media del número de saltos refleja un error del 3.8%.

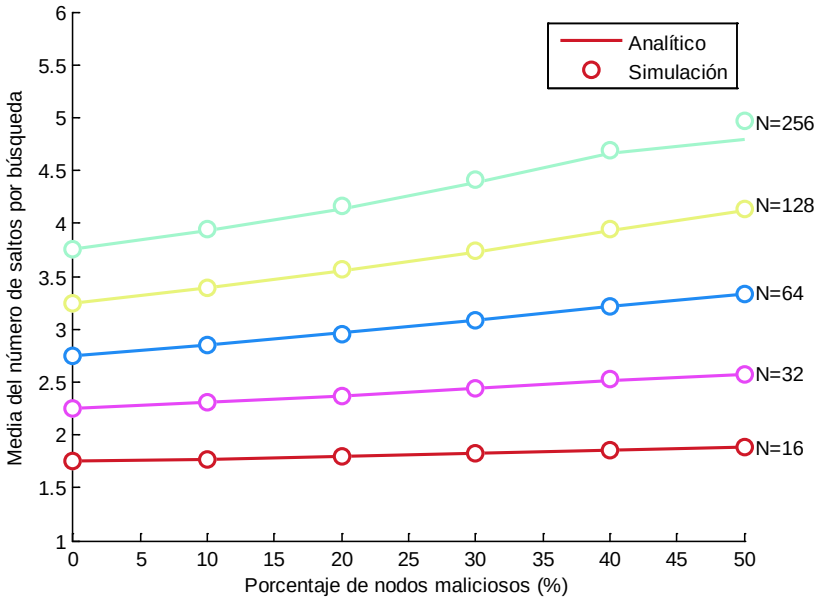


Figura 3.11. Resultados del modelo analítico contra los resultados de la simulación.

En la Figura 3.12 se ilustra el cambio en el desempeño del sistema con respecto a la media del número de saltos para Chord y para Chord-RELOAD. De la figura se puede ver que el protocolo RELOAD tiene una ligera mejora en cuanto a la media del número de saltos, debido a la inserción de 2 sucesores más en la tabla de enrutamiento. Cabe señalar, que en RELOAD el uso de los sucesores y los antecesores está pensado para incrementar la tolerancia a fallas del sistema, y la

diferencia que proporciona su uso en el enrutamiento aporta una ligera ventaja con respecto a Chord.

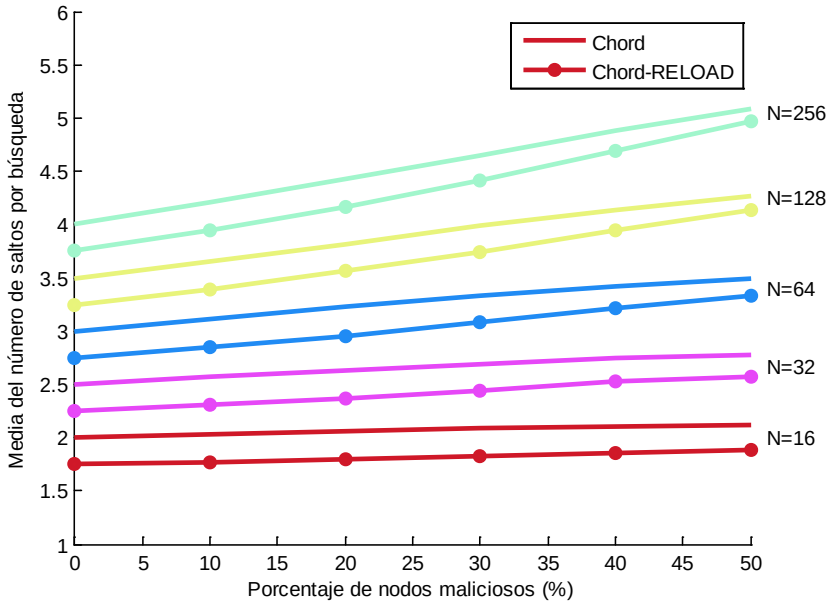


Figura 3.12. Comparativa entre Chord y Chord-RELOAD con respecto al número de saltos promedio.

La probabilidad de búsqueda exitosa se evalúa directamente a partir del algoritmo de trayectorias, incluyendo en el mismo a los sucesores adicionales que especifica el protocolo RELOAD. En la Figura 3.13 se muestra la verificación del método analítico por medio de la simulación de redes de nodos de tamaño variable, bajo la amenaza de nodos maliciosos. Asimismo, en la Figura 3.14 se hace una comparativa de redes de diferentes tamaños con diferentes porcentajes de nodos maliciosos con Chord y con Chord-RELOAD, en base a la probabilidad de que una búsqueda se complete.

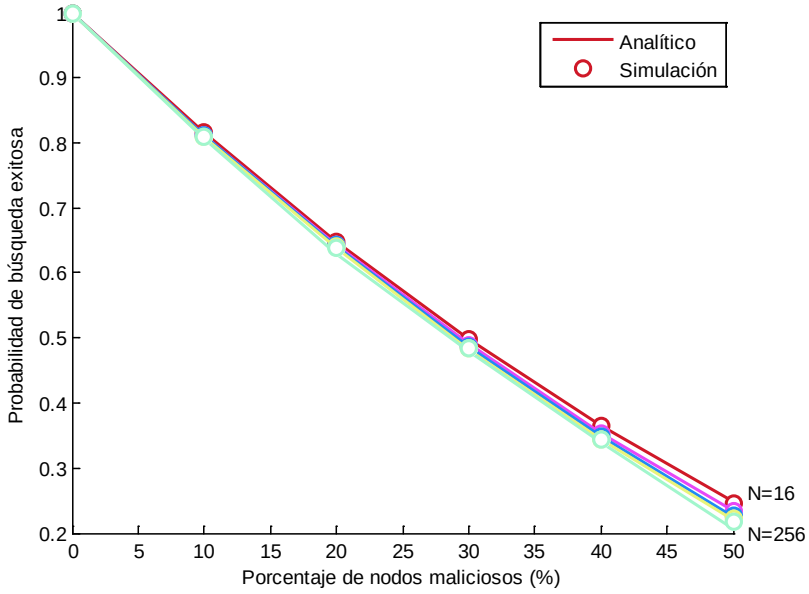


Figura 3.13. Probabilidad de búsqueda exitosa mediante el método analítico y por simulación.

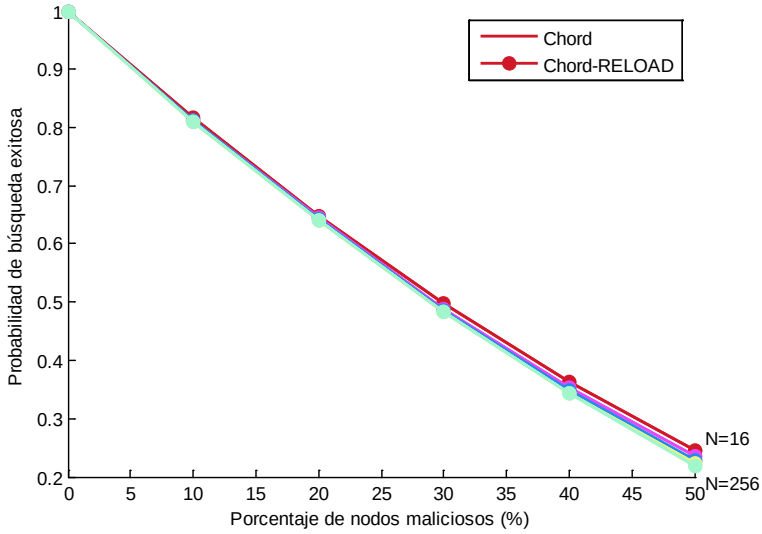


Figura 3.14. Comparativa entre Chord y Chord-RELOAD con respecto a la probabilidad de búsqueda exitosa.

Al examinar la Figura 3.12 y la Figura 3.14, se puede ver que la intervención de los sucesores en los procedimientos de enrutamiento no representa una gran diferencia en los parámetros de desempeño del sistema. Esto se debe a que sólo se está incrementando en uno el número de conexiones directas que se tienen en la tabla de enrutamiento, ya que tanto el primer como el segundo sucesor ya formaban parte de los dedos de un nodo y solamente se está anexando al tercer sucesor.

REFERENCIAS

[1] I. Stoica, R. Morris, D. Liben-Nowell, D. Karger, M. Kaashoek, F. Dabek y H. Balakrishnan, «Chord: a scalable peer-to-peer lookup protocol for Internet applications,» *IEEE/ACM Transactions on Networking,* vol. 11, nº 1, pp. 17-32, 2003.

[2] S. Ratnasamy, P. Francis, M. Handley, R. Karp y S. Shenker, «A scalable content-addressable network,» *Proceedings of the 2001 conference on Applications, technologies, architectures, and protocols for computer communications (SIGCOMM '01),* pp. 161-172, 2001.

[3] C. Jennings, B. Lowekamp, E. Rescorla, S. Baset y H. Schulzrinne, «REsource LOcation And Discovery (RELOAD),» *Rfc 6940,* 2014.

[4] S. Ratsanamy, *A scalable Content-Addressable Network,* PhD thesis, University of California at Berkeley, 2002.

[5] E. K. Lua, J. Crowcroft, M. Pias, R. Sharma y S. Lim, «A survey and comparison of peer-to-peer overlay network schemes,» *Communications Surveys & Tutorials, IEEE,* vol. 7, nº 2, pp. 72-93, 2006.

[6] J. Risson y T. Moors, «Survey of research towards robust peer-to-peer networks: search methods,» *Computer Networks: The International Journal of Computer and Telecommunications Networking,* vol. 50, nº 17, pp. 3485-3521, 2006.

[7] L. Jinyang, J. Stribling, R. Morris, M. F. Kaashoek y T. M. Gil, «A performance vs. cost framework for evaluating DHT design tradeoffs under churn,» *Proceedings of IEEE Infocom,* p. 13–17, 2005.

[8] K. Gummadi, R. Gummadi, S. Gribble, S. Ratnasamy, S. Shenker y I. Stoica, «The impact of DHT routing geometry on resilience and proximity,» *Proceedings of the 2003 conference*

on Applications, technologies, architectures, and protocols for computer communications, pp. 381-394, 2003.

[9] F. Chowdhury y M. Kolberg, «Performance Evaluation of Structured Peer-to-Peer Overlays for Use on Mobile Networks,» *2013 Sixth International Conference on Developments in eSystems Engineering (DeSE),* pp. 57-62, 2013.

[10] I. Baumgart y B. Heep, «Fast but economical: A simulative comparison of structured peer-to-peer systems,» *Proceedings of the 8th Euro-NF Conference on Next Generation Internet,* 2012.

[11] D. Germanus, R. Langenberg, A. Khelil y N. Suri, «Susceptibility Analysis of Structured P2P Systems to Localized Eclipse Attacks,» *2012 IEEE 31st Symposium on Reliable Distributed Systems (SRDS),* pp. 11-20, 2012.

[12] G. Urdaneta, G. Pierre y M. V. Steen, «A survey of DHT security techniques,» *ACM Computing Surveys,* 2011.

[13] M. Srivatsa y L. Liu, «Vulnerabilities and security threats in structured overlay networks: a quantitative analysis,» *20th Annual Computer Security Applications Conference,* pp. 252-261, 2004.

[14] D. Xuan, S. Chellappan y M. Krishnamoorthy, «RChord: an enhanced Chord system resilient to routing attacks,» *International Conference on Computer Networks and Mobile Computing,* pp. 253-260, 2003.

[15] C. Y. Lee, «Analysis of Switching Networks,» *Bell System Technical Journal,* vol. 34, nº 6, p. 1287–1315, 1955.

CAPÍTULO 4

4. EXTENSIÓN DE SEGURIDAD EN RELOAD

En este capítulo se estudian las vulnerabilidades del protocolo RELOAD en el módulo de topología de la red sobrepuesta ante la presencia de nodos malintencionados. Asimismo, se presentan mecanismos de defensa ante estas debilidades, representadas en la forma de escenarios de ataque propuestos. Finalmente, se introduce una propuesta de un mecanismo adicional de seguridad que permite mejorar y subsanar las flaquezas presentes en el actual protocolo RELOAD, para el procedimiento de inserción y recuperación de los objetos almacenados en el sistema distribuido.

4.1 INTRODUCCIÓN

El modelo de seguridad de RELOAD está basado en la propiedad de que cada uno de los nodos en la red cuenta con uno o varios certificados públicos. Estos certificados, así como los identificadores de cada nodo, son asignados por una entidad centralizada autorizada. El uso de certificados le permite a RELOAD ofrecer seguridad a 3 niveles:

- En las conexiones. Las conexiones directas entre nodos se aseguran con el uso de TLS o DTLS.
- En los mensajes. Cada mensaje que se intercambia se firma.

- En los objetos. Todos los objetos almacenados en la red sobrepuesta están firmados por el nodo que los almacenó.

Los 3 niveles de seguridad en conjunto, ayudan a que cualquier nodo dentro de la red pueda verificar el origen y la veracidad de la información que reciben de otros nodos. De una manera más específica, en RELOAD se tienen los siguientes mecanismos de defensa:

- Se asegura que todos los mensajes que se reciban provengan de miembros autorizados en la red por medio del uso de canales seguros. Estos proporcionan integridad de los mensajes y autenticación de las identidades de los pares en la comunicación.
- Los objetos en RELOAD se firman para proporcionar integridad de los mismos y se establecen políticas de acceso y manejo de los objetos dentro de la red sobrepuesta.
- En caso de utilizar el mecanismo de auto-certificación, se tiene una disminución en la seguridad proporcionada por RELOAD, debido a que se pueden presentar ataques Sybil, por lo que se recomienda su uso en configuraciones pequeñas donde todos los miembros de la red sobrepuesta sean de confianza.
- RELOAD también proporciona la opción del control de la admisión por medio de llave compartida, el cual es apropiado para redes pequeñas privadas.
- Los nodos tienen asignado un número máximo de objetos a almacenar para evitar ataques de negación de servicio.
- Para evitar ataques *version rollback* cada objeto tiene asignado un tiempo de vida y un tiempo de almacenamiento.
- Una entidad centralizada lleva el control de acceso a la red sobrepuesta, ésta asigna identificadores de manera aleatoria y limita la aparición de identidades Sybil dentro de la red.
- Para proteger el monitoreo de la señalización se utilizan canales seguros en las comunicaciones par a par (protección hacia el exterior de la red) y cada mensaje se firma (protección contra la alteración de los mensajes durante el enrutamiento).
- Se utilizan límites en los saltos dentro de la red para reducir el efecto de los ataques de re-direccionamiento durante el enrutamiento. Además, se supervisa que no exista ciclos en las listas de ruteo. No se tiene una contención completa contra los ciclos, pero limita en parte el comportamiento de los nodos maliciosos.

Sin embargo, a pesar de que se cuenta con la seguridad mencionada, aún pueden llegar a realizarse ataques cuando se encuentran algunos nodos maliciosos en un sistema que utilice RELOAD [1]. Los ataques residuales [12] presentes, pueden dividirse de acuerdo con el procedimiento al que afectan, es decir, los ataques enfocados al proceso de almacenamiento en la red y los ataques enfocados al proceso de enrutamiento de mensajes en el sistema. Cabe resaltar que en este trabajo solamente se estudian los ataques que pueden realizarse sobre el módulo de la topología de la red sobrepuesta, el estudio de ataques residuales en los demás módulos de RELOAD está afuera de los alcances de esta tesis.

Ataques residuales en el procedimiento de almacenamiento:

- Los nodos pueden negarse a almacenar los objetos enviando mensajes de error.
- Los nodos pueden negar la existencia de algún objeto previamente almacenado.
- Si se almacenan objetos multi-valuados, el nodo responsable podría entregar el objeto incompleto.

Ataques residuales en el enrutamiento:

- Si un nodo logra colocarse entre 2 pares de nodos A y B, puede hacer parecer que B no existe o está fallido.
- Re-direccionamiento de la búsqueda, mediante la falsificación de información de la red.
- Los nodos subversivos pueden regresar mensajes de error para bloquear el enrutamiento o detenerlo.

En la sección 3.3.4 se estudiaron de manera cuantitativa los efectos que tiene la presencia de nodos maliciosos en el desempeño del sistema y lo importante que resulta proteger la red de los ataques presentados bajo el modelo de adversarios referido. A pesar de que el desempeño de la red en cuanto a número de saltos se refiere, no se ve tan afectado por los ataques presentados en el enrutamiento, el porcentaje de búsquedas exitosas sí sufre un decremento considerable conforme aumenta la cantidad de nodos adversos en el sistema. Debido a lo anterior, en el presente trabajo se analiza el protocolo RELOAD para determinar las brechas referentes a la seguridad que proporciona. En este capítulo se proponen algunos escenarios de ataque en

[12] El término residual se refiere a aquellos ataques que pueden realizarse en el sistema, posteriores a la implementación de las medidas de seguridad referidas en el protocolo.

RELOAD, con el objetivo de estudiar el impacto que sufre el sistema bajo los mismos, así como determinar posibles soluciones que mitiguen sus efectos. Por último, tomando como referencia los escenarios de ataque formulados, se propone una solución que cubra las excepciones de seguridad que presenta una red RELOAD bajo la amenaza de nodos malintencionados.

4.2 ESCENARIOS DE ATAQUE

Los escenarios que se presentan a continuación son aquellos que resultan del estudio de las defensas de seguridad proporcionadas por el protocolo RELOAD y sus limitaciones. Al mismo tiempo, éstos están basados en ataques reportados en la literatura y han sido adecuados para su incorporación en un sistema basado en el RFC 6940[13], en el módulo de la topología de la red sobrepuesta. En este caso, la topología de la red sobrepuesta es una modificación del protocolo Chord, por lo que en lo siguiente, para su evaluación se emplean metodologías similares a las del capítulo anterior.

4.2.1 Escenario de ataque 1

En este escenario el nodo malicioso niega las peticiones hacia un recurso o hacia réplicas que almacenó previamente. Este ataque puede realizarse enviando mensajes de error cada vez que se solicite un objeto, ya que el protocolo sólo verifica que el nodo se encuentre en buen estado, a lo cual el nodo puede contestar de manera adecuada. Asimismo, si los nodos pertenecientes al conjunto de nodos-réplica, es decir los nodos que almacenan una copia del objeto además del responsable, son de naturaleza maliciosa, la consecuencia de un ataque de esta índole es que un recurso no se pueda recuperar.

La probabilidad de que recurso no pueda ser recuperado a partir del nodo responsable o de alguno de los nodos-réplica está dada por:

[13] Para una revisión de los ataques en sistemas P2P de los cuales se desprenden los aquí mencionados, referirse al capítulo 2.

$$P\{Los\ responsables\ de\ las\ réplicas\ son\ maliciosos\} = \left[\binom{N}{k} p^k q^{N-k}\right][f^k]$$

Donde:

Los *k* nodos maliciosos son responsables del objeto y de las réplicas.

Se considera una red de *N* nodos.

Dentro de un espacio de identificadores de tamaño *T*.

Se supone una fracción *f* de nodos maliciosos en la red.

Además, si se considera que $N \to \infty$, $T \to \infty$, el espacio entre 2 nodos definido por el intervalo $t_a = t_2 - t_1 \ll T$ y $\lambda = \frac{N}{T} = cte$, entonces la probabilidad queda dada por la aproximación bien conocida:

$$P\{Los\ responsables\ de\ las\ réplicas\ son\ maliciosos\} = \left[e^{-\lambda t_a} \frac{(\lambda t_a)^k}{k!}\right][f^k]$$

En la Figura 4.1 se muestra la probabilidad de que ocurra este escenario en función del número de réplicas en el conjunto de nodos-réplica y en función de del porcentaje de nodos maliciosos en la red.

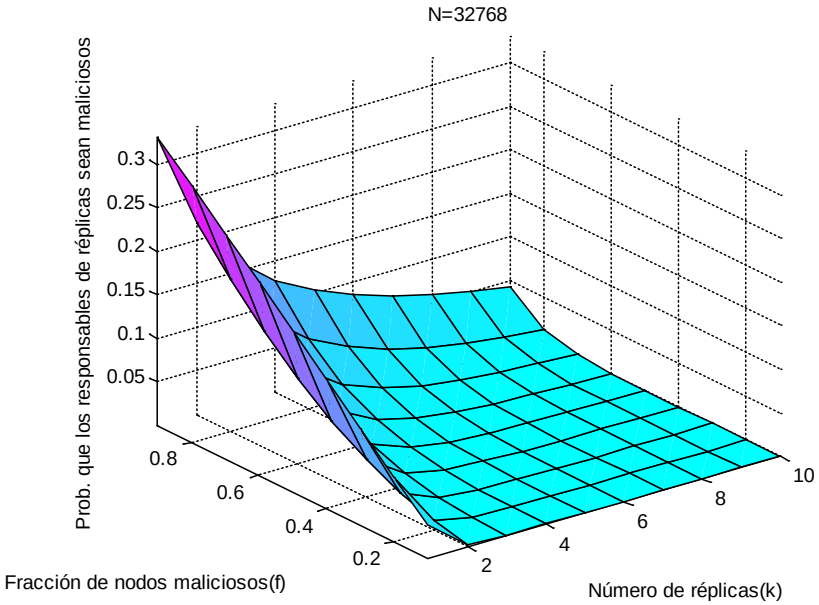


Figura 4.1. Probabilidad de que los nodos responsables de un objeto sean maliciosos.

Existen diversas formas de disminuir los alcances de un ataque de este tipo, se propone:

1. Almacenar el recurso en diferentes posiciones del anillo.

En este caso se pueden realizar búsquedas paralelas a los objetos, sin embargo se hace con el compromiso de incrementar el número de las peticiones de búsqueda, que se refleja en tráfico de la red, así como en la carga en los nodos. Pero, por otro lado, se asegura que con mayor probabilidad alguna copia del objeto llegará al solicitante. Además, otro aspecto a considerar es que durante la etapa de mantenimiento de la red, se debe asegurar el estado de las réplicas, es decir, todas las copias que existen en la red deben de ser idénticas. Si se implementa esta opción, la probabilidad de que el recurso no se recupere está dada por:

$$P\{No\ se\ puede\ acceder\ al\ recurso\} = \left\{\left[e^{-\lambda t_a}\frac{(\lambda t_a)^k}{k!}\right][f^k]\right\}^l$$

Donde:

$$l: Número\ de\ colocaciones\ en\ el\ anillo$$

2. Incrementar el número de réplicas.

Al realizar un incremento en el número de réplicas que se tiene de un objeto, es necesario evaluar la cantidad de recursos que convendría que un nodo almacenara. Ya que dependiendo del tamaño de la red y la ocupación de la misma, así como el tipo de objetos que se distribuyen en el sistema, el nodo podría requerir de almacenar un tamaño de información considerable. Esta solución presenta una probabilidad de que el recurso no se pueda obtener de:

$$P\{No\ se\ puede\ acceder\ al\ recurso\} = \left[e^{-\lambda t_a}\frac{(\lambda t_a)^k}{k!}\right][f^k]$$

Donde:

$$k: Número\ de\ réplicas$$

4.2.2 Escenario de ataque 2

En el protocolo RELOAD se especifica que el nodo responsable de almacenar el objeto es asimismo el encargado de enviar las copias a los nodos del conjunto de réplicas. Un nodo malicioso podría rehusarse a enviar las peticiones de almacenamiento a los nodos y además negar el recurso, con lo que el objeto no podría recuperarse.

La probabilidad de que ocurra este evento es:

$$P\{El\ recurso\ no\ puede\ obtenerse\} = f$$

En este caso, la probabilidad de que el recurso no sea recuperable es considerablemente mayor a comparación del escenario anterior, ya que va ligado a la porción de nodos maliciosos en el sistema. Para contrarrestar el impacto que tiene este ataque en la red se propone:

1. Tener distintos responsables de las réplicas.

   Esta solución conlleva a un incremento en los costos de almacenamiento de los nodos que almacenan las réplicas, así como en las peticiones de búsquedas de los recursos. Además, se requiere una modificación de la metodología de búsqueda que permita la realización ya sea de búsquedas de manera paralela o secuencial. Bajo esta implementación, la probabilidad de que un objeto no pueda recuperarse del sistema cae exponencialmente con respecto al número de responsables involucrados.

$$P\{El\ recurso\ no\ puede\ obtenerse\} = f^{l}$$

   Donde:

   l: $N\acute{u}mero\ de\ responsables$

2. El dueño del recurso realiza el almacenamiento en los nodos del conjunto de réplicas.

   Si el dueño del objeto es el que lo almacena en los nodos-réplica entonces se asegura que el nodo responsable evite su almacenamiento, sin embargo aún existe la posibilidad de que alguno de los nodos de este conjunto sea malicioso y se requiera realizar búsquedas posteriores. En este caso, los costos de mantenimiento de los objetos no se incrementan, pero

sí podrían aumentar los costos de las peticiones de búsqueda. La probabilidad de que el recurso no pueda obtenerse se ve limitada a:

$$P\{El\ recurso\ no\ puede\ obtenerse\} = \left[\binom{n}{k} p^k q^{n-k}\right][f^k]$$

Donde:

k: $Número\ de\ réplicas$

4.2.3 Escenario de ataque 3

En el protocolo Chord, todas las peticiones de búsqueda llegan hasta al nodo predecesor del objeto solicitado, por esta razón si el nodo predecesor es un nodo malicioso, todas las búsquedas que se realicen a su sucesor se verán afectadas y los recursos de los cuales sea responsable no podrán obtenerse. Si se supone una fracción de nodos maliciosos f en el sistema, la probabilidad de que el predecesor sea un nodo subversivo y la búsqueda sea fallida es:

$$P\{El\ recurso\ no\ pueda\ obtenerse\} = f$$

Para evitar la búsqueda fallida cuando los nodos malintencionados presentan este comportamiento, se propone:

1. Búsqueda bidireccional.

   Para mejorar el desempeño en la búsqueda algunos autores proponen el uso de un grafo bidireccional en contraposición con el grafo unidireccional de Chord [2]. En esta metodología se tiene una tabla de dedos espejo que se construye como un reflejo en el espacio de identificadores de los dedos de Chord original, la cual forma parte de la tabla de enrutamiento utilizada en el procedimiento de búsqueda. Además de introducir una mejora en la eficiencia de las búsquedas, esta técnica permite disminuir el impacto de un predecesor malicioso, pues se cuenta con un nodo predecesor espejo. Si se considera que los nodos son maliciosos de manera independiente, la probabilidad de que una búsqueda regrese un resultado negativo en este esquema está dada por:

$$P\{El\ recurso\ no\ puede\ obtenerse\} = f^2$$

2. Múltiples responsables de un recurso

Si se cuentan con varios nodos responsables para un mismo recurso, la probabilidad de que todos los nodos predecesores asociados sean maliciosos decrementa exponencialmente en base al número de predecesores determinados. Sin embargo, con el incremento de nodos responsables de un objeto, también existe un incremento en el costo de almacenamiento en cada nodo y en el tráfico asociado a las peticiones de búsqueda. Adicionalmente, se debe prestar especial cuidado en mantener la consistencia de los objetos, lo cual conlleva a un incremento de tráfico y de retardo en las etapas de mantenimiento de la red. Por último, se debe realizar una modificación en la metodología de búsqueda que indique el procedimiento a seguir cuando se deseen hacer búsquedas secuenciales o de manera paralela. Considerando que los nodos maliciosos actúan de manera independiente, la probabilidad de que un recurso no pueda recuperarse en un sistema que implemente esta protección es:

$$P\{El\ recurso\ no\ puede\ obtenerse\} = f^l$$

Donde:

l: $Número\ de\ responsables\ del\ objeto.$

4.2.4 Escenario de ataque 4

En este escenario, el nodo malicioso detiene el avance de las peticiones de búsqueda al proporcionar mensajes de error cuando le llegan. Este comportamiento provoca una disminución en el desempeño de las búsquedas puesto que una petición puede llegar a su destino en un número mayor de saltos. Además, es posible que existan búsquedas que no se completen, debido a la negación del recurso. Este escenario de ataque es analizado a mayor profundidad en la sección

3.3.4, de donde resulta que la probabilidad de que una búsqueda sea fallida para una red de N nodos es:

$$P\{Búsqueda\ fallida\} = 1 - \sum_{d=0}^{N-1} \sum_{i_d} f^{longitud_{i_d}} (1-f)^{saltos_{i_d}+1}$$

Donde:

i_d	$i_d = 1, \ldots., númeroDeTrayectorias(d)$
$númeroDeTrayectorias(d)$	Número de trayectorias de la distancia d
$longitud_{i_d}$	Número de nodos maliciosos en la trayectoria i_d
$saltos_{i_d}$	Número de saltos en la trayectoria i_d

La obtención del número de trayectorias así como del número de nodos maliciosos que se encuentran en una trayectoria dada, se realiza por medio del algoritmo de trayectorias de la sección 3.3.3.

El impacto de este ataque puede contrarrestarse con el uso de rutas alternativas. Idealmente, las rutas alternativas deberían de ser rutas independientes de tal forma que en 2 rutas entre un nodo origen y un nodo destino, sólo estos 2 nodos fueran común en cada ruta. Sin embargo, debido a la construcción del protocolo Chord, sólo es posible tener una ruta independiente, por lo que existen diversas opciones propuestas en la literatura para la construcción de rutas alternativas. Para la generación de rutas independientes adicionales en [3] se propone generar un anillo duplicado de tal forma que un objeto tenga dos rutas independientes. Siguiendo con la idea de la superposición de anillos para la creación de rutas independientes en [4] se evalúa una metodología para la creación de múltiples trayectorias basada en la generación de particiones inconexas del espacio de identificadores de Chord. Una solución que resulta directa para la creación de rutas alternativas es utilizar un esquema bidireccional como en [5]. Por otro lado, se podría modificar la metodología de asignación de identificadores de tal forma que a un recurso se le asignen múltiples identificadores repartidos sobre el espacio de identificadores, como se plantea en [6].

La utilización de rutas alternativas para el enrutamiento de las búsquedas en un ambiente malicioso, conlleva a un incremento en el costo de almacenamiento de las nuevas entradas de la tabla de enrutamiento, así como un incremento en el tráfico de la red y en el retardo para la recuperación de un objeto. Asimismo, si se utiliza el mecanismo de múltiples identificadores para un recurso, es necesario que en las fases de mantenimiento de la red se asegure la consistencia de los datos.

4.3 PROPUESTA DE ESQUEMA DE SEGURIDAD

En la sección anterior se presentaron escenarios probables de ataque en una red RELOAD, bajo la presencia de nodos maliciosos, donde se manipulan las vulnerabilidades presentes en los procedimientos de almacenamiento y enrutamiento en el módulo de la topología de la red. Además, se presentaron algunas soluciones que contrarrestan el efecto de los ataques residuales mencionados. Como se infirió en el capítulo 2 y en las secciones anteriores de este capítulo, las soluciones a las debilidades en la topología de la red sobrepuesta están basadas en el principio de almacenamiento y enrutamiento redundante. De manera general, en el almacenamiento redundante un objeto o recurso es guardado en diferentes lugares, de tal forma que cuando no es posible obtener una de las copias aún existan otras más en el sistema. De forma similar, en el enrutamiento redundante existen diferentes vías o rutas que permiten llegar desde un punto en la red hasta otro punto destino, así cuando alguno de los caminos se encuentra amenazado por la presencia de nodos maliciosos o bien por alguna falla, existen otras rutas alternativas para llegar al destino. La solución propuesta, está basada en el uso de los principios de redundancia sobre los procedimientos de almacenamiento y enrutamiento, como se detalla en las siguientes secciones.

4.3.1 Antecedentes de replicación

En los sistemas distribuidos existen diversas formas de realizar almacenamiento redundante y con diversos fines. En [7] se hace una clasificación de los mecanismos de replicación que se han utilizado en los sistemas de archivos distribuidos:

- Replicación aleatoria. Los nodos donde se replican los archivos son seleccionados de manera aleatoria.
- Replicación en el lado del servidor (*Server-end*). En este caso, los archivos se replican en nodos que están cercanos al dueño del archivo en la red sobrepuesta.
- Replicación en la ruta. Los archivos se replican en nodos distribuidos a través de la ruta de búsqueda del archivo original, con el fin de disminuir la longitud de ruta promedio del sistema.
- Replicación en el lado del cliente (*Client-end*). Si un nodo supera una cantidad de peticiones determinada para un objeto, se vuelve responsable de una copia del mismo.

A pesar de ser estos los mecanismos de replicación comúnmente implementados en los sistemas de distribución o compartición de archivos, existen otros esquemas de replicación enfocados a cumplir objetivos específicos. Un esquema de replicación puede distribuir las réplicas en base a la popularidad de los objetos, de tal forma que se disminuya el promedio global de retardo en las búsquedas, como se presenta en [8]. Asimismo, el esquema de replicación empleado permite adicionalmente mejorar alguna característica de la red, en [9] se propone un esquema que permite solucionar el problema de la disponibilidad de los datos así como el balance de la carga en cualquier tabla hash distribuida empleando árboles binarios. Otro parámetro de desempeño que puede mejorarse por medio de la metodología de replicación utilizada es el retardo asociado a los saltos que se realizan en la red subyacente durante una trayectoria en la red sobrepuesta. En [10] se organizan grupos de nodos de acuerdo con la proximidad física e intereses en común para un sistema de compartición de archivos, en los cuales se crean réplicas para mejorar la eficiencia de la búsqueda. En los sistemas distribuidos actuales donde la información almacenada ha pasado de ser estática a ser dinámica, es decir, los documentos y objetos que se insertan en la red cambian con el tiempo, es necesario asegurar la consistencia de los datos. La consistencia de la información se refiere a que cuando en un sistema existen diferentes copias de un objeto almacenadas en

distintas ubicaciones, al momento de que el objeto original es modificado, así mismo deben modificarse las copias. En [11] se hace un resumen de las técnicas de replicación que permiten asegurar la consistencia de los datos actualmente estudiadas. Finalmente, los esquemas de replicación utilizados en las redes *Peer-to-Peer* que requieren de almacenar grandes cantidades de información pueden auxiliarse de técnicas de fragmentación y codificación para mantener la disponibilidad de los datos y su persistencia, como se propone en [12] o en [13], donde se hace uso de códigos *erasure* o *rateless*. En estos esquemas se puede emplear la replicación redundante, donde el objeto original se copia en r diferentes nodos y donde además éste se puede fraccionar en k partes del mismo tamaño y cada k-ésima parte se reparte a un nodo del conjunto de r nodos. Asimismo, se puede emplear redundancia por *erasure code*, en la cual el objeto se expande por medio de una codificación, en la cual se divide en k partes y se tiene como resultado n partes ($k \geqslant 1, \quad n \geqslant k$), las cuales se reparten a nodos distintos. Para la recuperación del objeto original se requiere de cualquier subconjunto de k' partes ($k' \geqslant k$).

Todos los esquemas de replicación mencionados proporcionan mecanismos para asegurar el almacenamiento redundante, sin embargo, en un sistema afectado por la presencia de nodos maliciosos es necesario contar con un mecanismo que además proporcione rutas alternativas. En [14] se estudia la replicación como un mecanismo que incremente la robustez del enrutamiento al generar rutas disjuntas. Las copias de los objetos se distribuyen de manera uniforme es decir, igualmente espaciadas entre sí, de tal forma que las rutas hacia ellas cubran segmentos del anillo que no se traslapen entre sí, asegurando rutas con un menor número de nodos en común.

4.3.2 Esquema de seguridad propuesto

El objetivo del esquema de seguridad propuesto es brindar protección en una red RELOAD con nodos maliciosos presentes con el fin de mejorar la calidad del procedimiento de recuperación de objetos. El esquema presenta el uso de una función de replicación, que proporciona almacenamiento redundante y además proporciona rutas alternativas hacia un recurso dentro de la red sobrepuesta. Para la evaluación de la propuesta se recurre nuevamente[14] a los parámetros

[14] En el Capítulo 3 se explica con mayor profundidad porque se han elegido estos parámetros como medida de evaluación.

de desempeño: número de saltos y probabilidad de búsqueda exitosa. Estos parámetros se evalúan de manera analítica y se comprueba la validez de la metodología analítica por medio de una simulación.

En la propuesta se realiza replicación redundante donde el dueño realiza k copias del objeto a almacenar y las distribuye de manera uniforme sobre el anillo, de tal forma que de su objeto existen $k + 1$ reproducciones en el sistema. Al realizar la distribución de los objetos de esta manera se introducen las siguientes características de protección:

- Si un responsable de alguna copia del objeto es malicioso y niega la existencia del recurso, existen otras k copias que aseguran su disponibilidad. Conforme k aumenta, la probabilidad de que ninguna de las copias pueda ser recuperada del sistema disminuye de manera exponencial.
- Debido a que el dueño del recurso realiza la distribución de las réplicas, se anula la posibilidad de que el responsable no las distribuya hacia el conjunto de nodos-réplica. Cabe señalar que en RELOAD los objetos se replican en los 3 sucesores y los 3 antecesores de cada nodo responsable, esto con el fin de incrementar la tolerancia a fallas, por lo que aún existe la posibilidad de que algún nodo responsable sea malicioso y no las respalde en sus nodos vecinos. Sin embargo, al haber múltiples responsables se asegura con mayor probabilidad que el recurso se encuentre disponible.
- La replicación uniforme redundante brinda protección a ataques donde el nodo predecesor es un nodo subversivo, así como se disminuye la probabilidad de búsqueda fallida ante nodos adversos que detienen las peticiones de búsqueda; esto se debe a las rutas alternativas inherentes de este esquema.

A continuación se realiza el análisis para determinar la media de saltos de una búsqueda, en un sistema RELOAD utilizando el esquema de seguridad propuesto, considerando:

- El espacio de identificadores de la red es de tamaño 2^m , es decir, se utiliza un tamaño de identificador m.
- Repartidos en el anillo de la red se encuentran N pares.
- Los pares se encuentran uniformemente distribuidos sobre el anillo, distanciados entre ellos a una unidad.

- Los dedos de cada par están definidos de acuerdo con:

$$dedo_i = sucesor\left(\left(id + 2^{i-1}\right) mod\ 2^m\right) \quad ; \quad 1 \leq i \leq m$$

- Cada objeto es almacenado k veces de manera uniforme en el anillo.
- La probabilidad de que un nodo sea malicioso es f.
- La probabilidad de que un nodo sea malicioso es independiente, es decir, no existen las coaliciones de nodos malintencionados.
- El nodo subversivo no dirige ninguna petición de búsqueda hacia el siguiente salto.
- Un nodo malicioso no puede elegir su ubicación en el anillo, puesto que su identificador es asignado de acuerdo con el protocolo y sólo le es asignado una vez.
- Cuando el nodo malicioso es responsable de un objeto o es el último salto, no es posible la recuperación del objeto.

El parámetro de desempeño que se desea encontrar es la media de la variable aleatoria *número de saltos*, desde un nodo origen a un nodo destino cualesquiera dentro de la red sobrepuesta, cuando existe una fracción f de nodos maliciosos en el anillo, es decir:

$$\mathbb{E}\{\mathcal{S}\} \quad ; \quad \mathcal{S}\colon\ v.a.\text{número de saltos}$$

El análisis se realiza basado en los saltos a los cuales un par origen se encuentra del par destino y a la distancia (en número de pares) a la que están dentro del anillo. Para llevar a cabo los saltos, el nodo cuenta con una tabla de enrutamiento donde están incluidos sus m dedos. A partir de la tabla de enrutamiento, un nodo ocupa aquel dedo que le acerque más al nodo deseado, siempre que esta opción sea confiable. En la evaluación del sistema se supone que se realizan búsquedas a cada una de las $k + 1$ copias del recurso.

Partiendo de la media de saltos para un anillo de tamaño N, dada por[15]:

$$\mathbb{E}\{\mathcal{S}\} = \frac{1}{N}\sum_{d=0}^{N-1}\sum_{i} s_i P\{\mathcal{S} = s|\mathcal{D} = d\} = \frac{1}{N}\sum_{d=0}^{N-1}\mathbb{E}\{S|\mathcal{D} = d\}$$

[15] Revisar sección 3.2

Nombrando, la media de saltos para una búsqueda exitosa dado que se encuentra a una distancia d, como:

$$\mathbb{E}\{S|\mathcal{D} = d\} = s(d)$$

La cual se puede encontrar por medio del algoritmo de trayectorias de la sección 3.3.3, por medio del cual se pueden evaluar las trayectorias obtenidas por el mismo para cada d, de la siguiente forma:

$$s(d) = \frac{\sum_i saltos_i f^{longitud_i}(1-f)^{saltos_i+1}}{\sum_i f^{longitud_i}(1-f)^{saltos_i+1}}$$

Donde:

i	$i = 1, \ldots, númeroDeTrayectorias(d)$
$númeroDeTrayectorias(d)$	Número de trayectorias de la distancia d
$saltos_i$	Número de saltos en la trayectoria i
$longitud_i$	Número de nodos maliciosos en la trayectoria i

Para un número de k réplicas uniformemente espaciadas en el anillo de N nodos, la media de saltos está dada por:

$$\mathbb{E}\{S_k\} = \frac{1}{N}\sum_{d=0}^{N-1} \mathbb{E}\{S_k|\mathcal{D} = d\}$$

De igual manera, renombrando la media de saltos para una búsqueda exitosa dado que se encuentra a una distancia d, como:

$$\mathbb{E}\{S_k|\mathcal{D} = d\} = s_k(d)$$

Donde:

$$s_k(d) = \begin{cases} 0 & ; s\left(d + \frac{iN}{k}\right) = s(0) \\ \frac{\sum_{i=0}^{k-1} s\left(d + \frac{iN}{k}\right) f^i (1-f)^2}{\sum_{i=0}^{k-1} f^i (1-f)^2} & ; otro \end{cases}$$

Bajo la suposición que las búsquedas se realizan de manera paralela, se considera que la trayectoria con mayor probabilidad será aquella que realice el mínimo de saltos.

Para la verificación del modelo analítico se compararon los resultados del método analítico y los de una simulación, haciendo variar el tamaño del anillo y la proporción de nodos maliciosos en el sistema. En la Figura 4.2 se ilustra la comparación para un factor de replicación de dos y en la Figura 4.3 se muestra para un factor de replicación de 4.

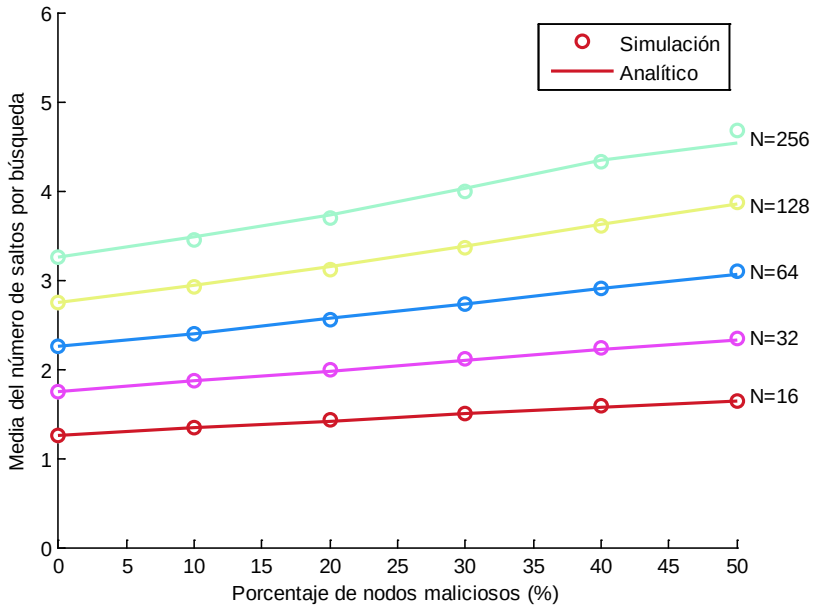


Figura 4.2. Validación del modelo analítico a través de simulación, para cuando existen 2 copias de un objeto en el sistema.

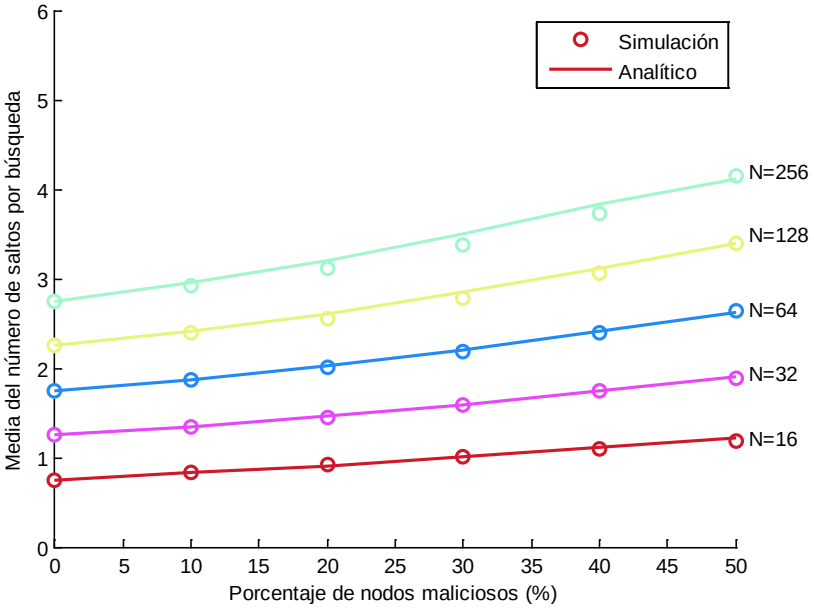


Figura 4.3. Validación del modelo analítico a través de simulación, para cuando existen 4 copias de un objeto en el sistema.

De las Figuras 4.2 y 4.3 se puede observar que el método analítico coincide con los resultados de la simulación, a excepción de la red de tamaño $N = 256$ para un 50% de nodos maliciosos, donde se observa que los resultados no son del todo coincidentes. Esta discordancia se debe a que, como se explicó en el capítulo 3, el algoritmo de generación de trayectorias no contabilizó algunas trayectorias cuya aportación al promedio estuviera por debajo de un rango establecido, sin embargo al ser un gran número de trayectorias las que cumplían con esta condición, el algoritmo presenta un error de truncado mínimo.

El segundo parámetro de desempeño analizado es la probabilidad de búsqueda exitosa, la cual se puede obtener de manera directa del algoritmo generador de trayectorias, a partir de:

$$Probilidad\ búsqueda\ exitosa = \sum_{d=0}^{N-1} \sum_{i_d} f^{longitud_{i_d}} (1-f)^{saltos_{i_d}+1}$$

Donde:

i_d	$i_d = 1, \ldots., númeroDeTrayectorias(d)$
$númeroDeTrayectorias(d)$	Número de trayectorias de la distancia d

$longitud_{i_d}$ Número de nodos maliciosos en la trayectoria i_d

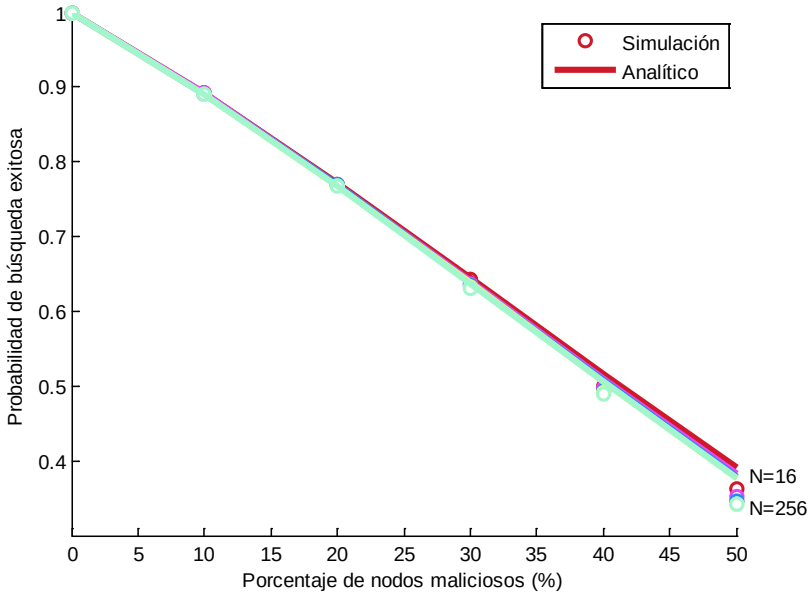


Figura 4.4. Probabilidad de búsqueda exitosa, resultados del modelo analítico y de la red simulada, cuando en la red existen 2 copias de un recurso.

En la Figura 4.4 se muestra la probabilidad de búsqueda exitosa derivada del modelo analítico y la derivada de la simulación para un factor de replicación de dos y en la Figura 4.5 para un factor de replicación de 4. En estas se varían el tamaño de la red y el porcentaje de nodos maliciosos presentes en el sistema.

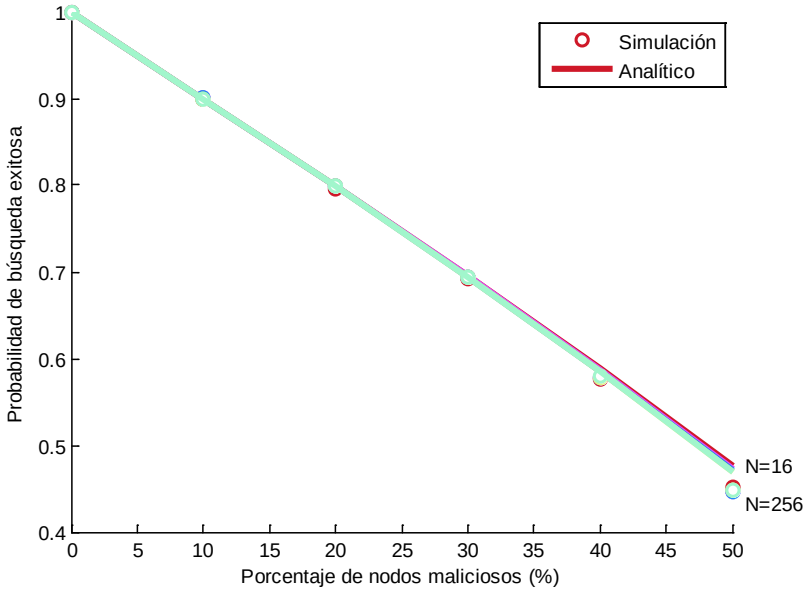


Figura 4.5. Probabilidad de búsqueda exitosa, resultados del modelo analítico y de la red simulada, cuando en la red existen 4 copias de un recurso.

En las Figuras 4.4 y 4.5 se puede apreciar con mayor claridad el error introducido por el truncamiento de la adición de trayectorias cuando la fracción de nodos maliciosos es del 50%. Sin embargo, el modelo analítico aún con el recorte de trayectorias presenta una aproximación muy cercana a los resultados de la simulación.

Por último, se presenta el desempeño de un sistema RELOAD antes y después de haber implementado el esquema de seguridad propuesto con 2 y 4 copias de los objetos en un anillo de tamaño N=128.

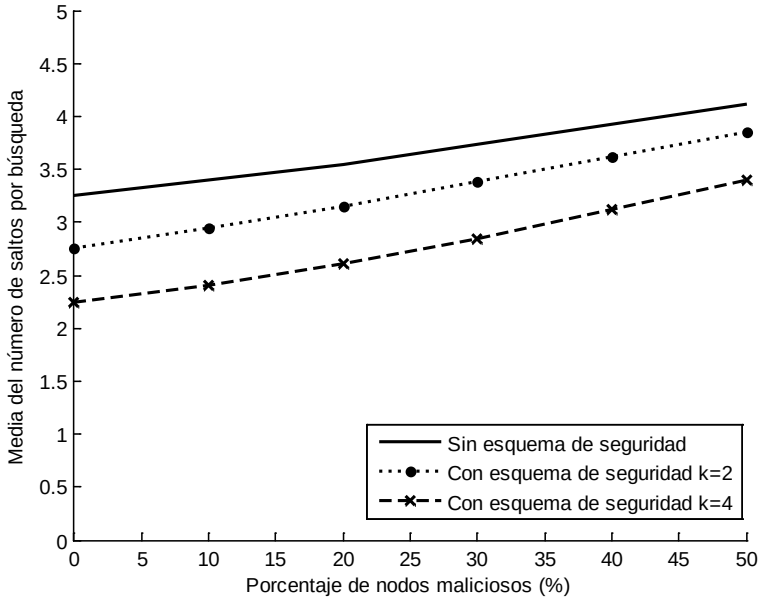


Figura 4.6. Media del número de saltos en una red RELOAD antes y después del esquema de seguridad propuesta.

En las Figuras 4.6 y 4.7 se muestra la mejora que presenta el sistema cuando se le incorpora el método de seguridad propuesto. En relación a la media del número de saltos por búsqueda, se tiene una mejora del 30% cuando no se tienen nodos maliciosos en la red y del 18% cuando la red se encuentra bajo una amenaza de proporción 2:1 (nodos adversos contra nodos integrales), cuando en el anillo existen 4 copias de un recurso. De manera aproximada, se tiene una disminución de un salto en el promedio general cuando se utiliza la replicación redundante con $k = 4$. Por otro lado, la probabilidad de búsqueda exitosa se ve afectada en gran medida cuando no se tiene ningún mecanismo de defensa adicional a los establecidos en el protocolo RELOAD, numéricamente en promedio solo el 20% de las peticiones de búsquedas hacia un objeto tienen un resultado positivo con un 50% de nodos maliciosos. En cambio, cuando solamente se introducen 3 copias adicionales de un objeto en el anillo, la probabilidad de búsqueda exitosa asciende un 125% del resultado original. Cabe destacar que conforme el número de réplicas se incrementa, la probabilidad de búsqueda exitosa se acerca al límite superior f, es decir, a pesar de que existan una gran cantidad de réplicas en el sistema, la búsqueda va a tener un resultado negativo si el nodo responsable es malicioso. Esto se debe a que en el límite cuando todos los nodos dentro de anillo tienen una copia de todos los objetos almacenados, entonces la

probabilidad de recuperar un objeto, buscándolo en cualquier nodo del sistema, es la probabilidad de que el nodo en cuestión sea malicioso.

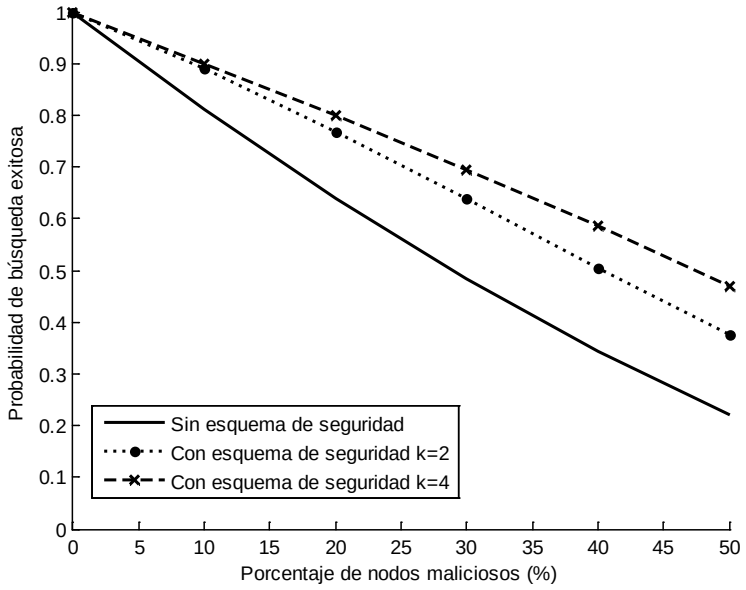


Figura 4.7. Probabilidad de búsqueda exitosa en una red RELOAD antes y después del esquema de seguridad propuesta.

REFERENCIAS

[1] C. Jennings, B. Lowekamp, E. Rescorla, S. Baset y H. Schulzrinne, «REsource LOcation And Discovery (RELOAD),» *Rfc 6940,* 2014.

[2] J. Jiang, R. Pan, C. Liang y W. Wang, «Bichord: An improved approach for lookup routing in chord,» *Advances in Databases and Information Systems,* pp. 338-348, 2005.

[3] Y. Mashimo, S. Ueda, Y. Shinzaki y H. Shigeno, «Examination of Forwarding Obstruction Attacks in Structured Overlay Networks,» *Third International Conference on Availability, Reliability and Security,* pp. 1340-1345, 2008.

[4] M. Artigas, P. Lopez y A. Skarmeta, «A novel methodology for constructing secure multipath overlays,» *IEEE Internet Computing,* vol. 9, nº 6, pp. 50-57, 2005.

[5] D. Xuan, S. Chellappan y M. Krishnamoorthy, «RChord: an enhanced Chord system resilient to routing attacks,» *International Conference on Computer Networks and Mobile Computing,* pp. 253-260, 2003.

[6] H. Kwon, S. Koh, J. Nah y J. Jang, «The Secure Routing Mechanism for DHT-based Overlay Network,» *International Conference on Advanced Communication Technology,* vol. 2, pp. 1300-1303, 2008.

[7] H. Shen, G. Liu y H. Chandler, «Swarm Intelligence Based File Replication and Consistency Maintenance in Structured P2P File Sharing Systems,» *IEEE Transactions on Computers,* vol. 64, nº 10, pp. 2953-2967, 2015.

[8] W. Rao, L. Chen, A. Fu y G. Wang, «Optimal Resource Placement in Structured Peer-to-Peer Networks,» *IEEE Transactions on Parallel and Distributed Systems,* vol. 21, nº 7, pp. 1011-1026, 2010.

[9] J. Li, J. Zhang, Z. Cao y W. Pei, «GenRe: A General Replication Scheme over an Abstraction of DHTs,» *Computer Software and Applications Conference,* pp. 43-52, 2013.

[10] H. Shen, G. Liu y L. Ward, «A Proximity-Aware Interest-Clustered P2P File Sharing System,» *IEEE Transactions on Parallel and Distributed Systems,* vol. 26, nº 6, pp. 1509-1523, 2015.

[11] E. Spaho, A. Barolli, F. Xhafa y L. Barolli, «P2P Data Replication: Techniques and Applications,» *Modeling and Processing for Next-Generation Big-Data Technologies,* pp. 145-166, 2015.

[12] R. Friedman, Y. Kantor y A. Kantor, «Replicated erasure codes for storage and repair-traffic efficiency,» *14-th IEEE International Conference on Peer-to-Peer Computing (P2P),* pp. 1-10, 2014.

[13] H. Ribeiro y E. Anceaume, «Exploiting Rateless Coding in Structured Overlays to Achieve Data Persistence,» *24th IEEE International Conference on Advanced Information Networking and Applications (AINA),* pp. 1165-1172, 2010.

[14] C. Harvesf y D. Blough, «The Effect of Replica Placement on Routing Robustness in Distributed Hash Tables,» *Sixth IEEE International Conference on Peer-to-Peer Computing,* pp. 57-66, 2006.

CONCLUSIONES

En el modelo cliente/servidor, máquinas con grandes capacidades de almacenamiento y procesamiento (servidores) son las encargadas de recibir y procesar los servicios de los usuarios de una aplicación (clientes). A diferencia de este modelo, en el modelo *Peer-to-Peer* (P2P) los usuarios o nodos actúan de ambas formas, de cliente y de servidor; de esta manera simultáneamente pueden solicitar o brindar alguna información hacia otros pares en el sistema. Adicionalmente, en la arquitectura P2P, los usuarios de una red comparten sus recursos con los demás participantes del sistema, como por ejemplo: recursos de almacenamiento, de procesamiento, periféricos, etc. Estos recursos compartidos pueden utilizarse para almacenar información de otros usuarios, para ejecutar aplicaciones que requieren de mucho procesamiento de manera distribuida, como puentes para la comunicación de usuarios en redes de gran escala, o simplemente para realizar las funciones inherentes de la propia red.

Las redes P2P lograron su popularidad con la aparición de Napster, la cual era una aplicación para la compartición de música. Posteriormente surgieron aplicaciones que consolidaron la tecnología P2P para la compartición de archivos, como Gnutella y BitTorrent. Actualmente, el esquema P2P ha evolucionado para brindar servicios distribuidos con una gran cantidad de usuarios mundialmente. Ejemplos de estas aplicaciones son PayPal, con un número de usuarios superior a 179 millones de usuarios y con 10 millones de transacciones al día; Bitcoin, que es otra aplicación de transacciones basada en el paradigma P2P, cuenta con aproximadamente 3 millones de usuarios globalmente; Skype, cuyo modelo, basado en P2PSIP, para la comunicación multimedia a través de la Internet aloja a 300 millones de usuarios ;o la aplicación Hola, cuya red *Peer-to-Peer* brinda servicios de tipo red virtual privada (VPN, Virtual private network) a más de 61 millones de usuarios.

La seguridad es un factor importante cuando se quieren realizar aplicaciones cuyos servicios interactúen con un gran número de usuarios, lo cual es cierto para aplicaciones del tipo cliente-servidor y para las aplicaciones de tipo *Peer-to-Peer*. En el caso de las redes P2P donde los usuarios tienen el control de información y de los recursos, tanto de otros usuarios como de la

red en sí, es imprescindible contar con cierto nivel de seguridad que asegure la integridad de los recursos y su buena administración. El nivel de seguridad que podrá proporcionar una red P2P está íntimamente ligado con el comportamiento que presentan los usuarios de la red, ya que si estos se comportan de una manera maliciosa, por ejemplo modificando la información del sistema, resulta complicado poder brindar niveles de seguridad similares a los de una aplicación centralizada similar. Adicionalmente, este nivel de seguridad proporcionado por la red, dependerá del número de nodos que actúen malintencionadamente. Por ejemplo, si un usuario malicioso quisiera atacar un recurso determinado, en una red P2P resulta complicado debido a su naturaleza distribuida, sin embargo, si la cantidad de usuarios que ataca el mismo recurso incrementa, la posibilidad de daño es mucho mayor.

El esquema P2P presenta amenazas de seguridad que son propias de los servicios distribuidos, como la negación de servicio distribuida, pero existen otras amenazas aplicables a otras arquitecturas cuyo resultado en el esquema par-a-par es intensificado. Estas amenazas o ataques son los referentes a las funciones de almacenamiento y enrutamiento del sistema P2P. En un sistema P2P, los mensajes o peticiones de servicio, deben de pasar por un conjunto de nodos intermedios para llegar al nodo destinatario. Estos nodos intermedios pueden realizar ataques en la ruta de búsqueda, como son la desviación de mensajes, la alteración de mensajes o la eliminación de peticiones. En cuanto a los procedimientos de almacenamiento, en una red P2P los nodos almacenan información de otros usuarios, pero sí un nodo malicioso se niega a almacenar el recurso o niega su existencia, el objeto no podrá recuperarse.

La justificación del trabajo realizado era precisamente entender el paradigma P2P y la importancia que tiene la seguridad en este tipo de redes. En base a lo cual, se puede concluir para cada capítulo lo siguiente:

- Capítulo 1. En este capítulo se revisaron los conceptos que conforman las redes P2P, el uso de las de las redes sobrepuestas para la organización de los usuarios en el sistema, así como para la asignación de responsabilidades en el entorno P2P. Para poder entender las bases de las redes par-a-par modernas se estudiaron 2 de los principales esquemas de redes sobrepuestas estructuradas utilizados actualmente: Chord y CAN. A partir de la revisión realizada, se pueden entender otros esquemas basados en las topologías de los

esquemas estudiados, como por ejemplo el caso del protocolo de señalización para redes P2P, RELOAD, el cual implementa una modificación de Chord.

- Capítulo 2. Las vulnerabilidades que presentan las redes P2P en cuanto la seguridad fueron revisadas en este capítulo, con lo cual es posible entender los alcances y limitaciones que surgen en una red P2P con usuarios subversivos. La revisión incluida en este capítulo incluye los ataques encontrados en la literatura comúnmente realizados en redes de este tipo. Sin embargo, aún existen problemas o brechas de seguridad que han ido surgiendo con la evolución del esquema P2P y que no se han revisado a fondo en la literatura. Muchas de estas vulnerabilidades están ligadas a las aplicaciones del paradigma distribuido, por ejemplo las referentes a los ataques en redes de transacciones financieras distribuidas, al anonimato en redes sociales y de cooperación distribuida, o a los ataques localizados en redes P2P consientes de la topología subyacente, entre otros.
- Capítulo 3. En este capítulo se evaluaron los protocolos de la red sobrepuesta, Chord y CAN, enfocando su evaluación en el procedimiento de búsqueda de un objeto dentro de la red, lo que permitió tener otro parámetro de comparación entre estas dos propuestas. Adicionalmente, se realizó un estudio del desempeño de una red bajo la presencia de nodos maliciosos, en términos de la media del número de saltos para una búsqueda exitosa y la probabilidad de búsqueda exitosa. En este estudio, se consideró que el comportamiento de los nodos era independiente, es decir, no existían coaliciones de nodos que actuaran con un fin común. Esta consideración se realizó en base a que bajo el escenario de evaluación no existía razón alguna por la cual la unión de los nodos resultara ventajosa. Cabe señalar que esta consideración no es adecuada en esquemas que utilizan redes de confianza o de reputación, donde los nodos enrutan las peticiones de búsqueda de manera segura, basados en puntuaciones del nivel de malicia en los nodos. En estos esquemas, la calificación de un nodo es resultado de las interacciones con otros usuarios en la red, por lo que un conjunto de nodos maliciosos puede favorecer a uno o varios nodos.

  En el capítulo se propuso un análisis probabilístico para encontrar los parámetros de desempeño requeridos, el cual fue evaluado por medio de un algoritmo debido a que no se pudo encontrar una expresión cerrada que reflejara la situación del sistema. En la literatura se encuentran soluciones que muestran la probabilidad de búsqueda exitosa

como umbrales numéricos superiores o inferiores, sin embargo no se define una solución que pudiese arrojar una solución numérica. Adicionalmente, en la literatura se encuentran múltiples resultados de la media del número de saltos para una búsqueda en presencia de nodos maliciosos, pero la mayoría de estos resultados se obtienen por medio de simulación y aquellos que presentan un modelo matemático no se ajustan a los resultados obtenidos por simulación. Como aportación de esta tesis, el análisis probabilístico propuesto proporciona una solución que no es solamente un valor umbral, sino un valor numérico, el cual además se valida con los resultados de la simulación.

- Capítulo 4. Basados en los ataques presentados en el Capítulo 2, se hizo un estudio de ataques propuestos que se podrían realizar en una red P2P que utilice el protocolo de señalización RELOAD, aún bajo el esquema de seguridad incluido en éste. Estos ataques residuales se revisaron para entender el alcance e impacto que tienen en el sistema, así como algunas de las soluciones que se podrían implementar para su mitigación. Si bien los ataques propuestos están basados en aquellos ataques referidos en la literatura, es posible que existan otros que sean modificaciones o combinaciones de los mismos, los cuales dependerán de la inventiva del atacante y de los recursos con los que cuente.

  Adicionalmente, en el capítulo se propone una solución integral que permite limitar el impacto que generan los ataques residuales mencionados. Esta solución está basada en técnicas de almacenamiento y enrutamiento redundantes, con el fin de minimizar las consecuencias negativas impuestas por la presencia de nodos maliciosos en la red. A pesar de que la solución propuesta mejora el desempeño del sistema con relación al procedimiento de búsqueda, existen otros factores que se deben de tomar en consideración para su implementación. Estos factores son principalmente los costos de la replicación, en cuanto a almacenamiento, o en cuanto al incremento del tráfico de la red cuando se realizan las búsquedas y cuando se realizan las operaciones de mantenimiento. También se debe de considerar el tipo de objeto a almacenar y su tamaño, puesto que de esto dependerá si es necesario implementar métodos de fragmentación, así como los procedimientos requeridos para mantener la consistencia en los datos. Por último, es necesario evaluar si es adecuado el uso de búsquedas paralelas o de búsquedas secuenciales para la recuperación de las réplicas.

De la revisión realizada en esta tesis, de la seguridad en redes P2P bajo la presencia de nodos maliciosos, se desprende el siguiente trabajo a futuro:

- En la tesis se presentan 2 de los esquemas de redes sobrepuestas comúnmente utilizados: Chord y CAN, pero en la actualidad existen otros esquemas que podrían analizarse e integrarse en la comparativa.
- Como ya se mencionó en este trabajo se realizó una revisión de los ataques presentes en los procedimientos involucrados para la realización de una búsqueda, sin embargo, existen otras ramas de estudio que no se abordaron. Algunas de estas ramas, son la integridad de los datos, la negación de servicio distribuida, los ataques a los nodos *bootstrap*, los ataques referentes a las aplicaciones particulares como P2PSIP, *streaming* P2P, etc.
- Uno de los campos que está siendo ampliamente estudiado en términos de la seguridad en redes P2P es el de las redes de reputación y confianza, el cual podría brindar otra perspectiva de solución a los ataques presentes en estos sistemas.
- Finalmente, el área de replicación en sistemas distribuidos es un área en continua expansión y de gran trayectoria, en esta tesis sólo se abordó una pequeña fracción de lo que estas técnicas aportan, por lo que es conveniente profundizar en algunas de las técnicas más avanzadas con el objetivo de solucionar los problemas de seguridad en las redes *Peer-to-Peer*.