Alta disponibilidad en redes ASON/GMPLS

Luis Velasco, Salvatore Spadaro, Jaume Comellas, Gabriel Junyent
Grupo de Comunicaciones Ópticas, Universidad Politécnica de Cataluña (UPC)
C/ Jordi Girona, 1-3, 08034 Barcelona España
Tel: +34 93 401 69 99, Fax: +34 93 401 71 02
{luis.velasco, spadaro, comellas, junyent}@tsc.upc.edu

Resumen

El presente artículo se centra en el estudio de la disponibilidad como función de la duración media de las conexiones en redes ASON/GMPLS y propone un nuevo algoritmo de enrutamiento diverso, que denominaremos FAR, que mejora la disponibilidad de las conexiones. Las conexiones estarán protegidas utilizando el esquema de protección de camino dedicado (DPP). El algoritmo FAR se comparará con otros dos algoritmos de enrutamiento diverso, todos basados en un algoritmo general. Los algoritmos difieren entre sí en el uso de la información sobre los fallos en la red.
Mediante simulación, se evaluará el comportamiento de los algoritmos en términos de probabilidad de bloqueo y disponibilidad. Por último, se definirá el concepto de duración umbral de las conexiones (THT) calculando su valor mediante simulación.

1. Introducción

La introducción de inteligencia en redes ASON [1] utilizando un plano de control GMPLS [2], permite el establecimiento, configuración y liberación de canales ópticos (lightpaths) en milisegundos. Automatizar la provisión reducirá significativamente la intervención manual y los costes involucrados (OPEX) en la manipulación de conexiones. Los datos de red, los comandos de configuración y las confirmaciones son creados automáticamente e intercambiados mediante protocolos de señalización y enrutamiento. Las capas de red clientes (IP, SDH, etc.) pueden solicitar conexiones ópticas a través de la interfaz estándar UNI [3]. Para permitir una entrega automatizada del servicio, ejecutado sin la más mínima intervención humana, se deberán negociar acuerdos de nivel de servicio entre el operador de red y los clientes.

La provisión de ancho de banda de forma rápida, abre nuevas oportunidades relacionadas con la mejor utilización de recursos, entrega de nuevos servicios como ancho de banda bajo de manda, y una amplia variedad de mecanismos de ingeniería de tráfico [4]. Las redes de transporte ópticas proporcionan una enorme cantidad de ancho de banda en cada *lightpath* establecido entre dos localizaciones. En la actualidad, el ancho de banda que requieren los clientes de la red es, normalmente, mucho menor que la capacidad de los *lightpaths*. Por ello, y para mejorar la utilización del ancho de banda, es necesario agrupar diferentes demandas entre las dos localizaciones. De esta forma, la gran mayoría de los *lightpaths* son conexiones permanentes o *soft-permanentes* (en ambos casos pueden ser establecidas mediante un sistema de gestión de la red).

La forma de mejorar la disponibilidad en las redes de transporte ópticas, es mediante el uso de esquemas de protección o restauración, de forma que pueda continuar en operación incluso en caso de fallos dentro de la red. Los mecanismos de protección se basan en reemplazar un recurso en fallo (por ejemplo, un enlace o un lightpath) con otro recurso preasignado. Los mecanismos de restauración se basan en el reenrutamiento utilizando capacidad de reserva. En ambos casos, los recursos de protección o de reserva pueden ser *dedicados*, en cuyo caso el recurso de reserva está dedicado a un único recurso de trabajo, o *compartidos*, donde el mismo recurso de reserva puede proporcionar protección a múltiples recursos de trabajo. Puede encontrarse una revisión más detallada de los esquemas de protección y restauración existentes en [5].

Dos diferentes esquemas de protección han sido propuestos, el esquema 1+1 y el 1:1. En protección 1+1, el nodo origen transmite simultáneamente tanto por los lightpaths de trabajo como de protección. El nodo destino monitoriza ambos lightpaths, escogiendo de forma dinámica la mejor señal. Si se detecta degradación en la señal del lightpath de trabajo, el nodo destino conmuta inmediatamente al lightpath de protección. En protección 1:1, el lightpath de protección se utiliza para transmitir tráfico de baja prioridad. Cuando se produce un fallo en el lightpath de trabajo, tanto el nodo origen como el de destino, conmutan al lightpath de protección, eliminando el tráfico de baja prioridad. La protección dedicada 1+1 es muy rápida (del orden de milisegundos) [6], robusta en caso de múltiples fallos y requiere un bajo grado de complejidad, sin embargo, no utiliza eficientemente los recursos de protección.

El escenario actual está cambiando rápidamente, el tráfico a ser transportado por las redes actuales de transporte se incrementa de forma muy rápida debido al uso masivo de aplicaciones de Internet y multimedia. De hecho, la diferencia entre la capacidad de transporte y el ancho de banda solicitado por los clientes está disminuyendo y la necesidad de establecer lightpaths bajo demanda en la forma de conexiones conmutadas se incrementa. Esto implica que la duración del servicio (el tiempo en que el cliente tiene establecida una conexión) será progresivamente más corto, desde años y meses a días e incluso horas. Además, el tiempo de establecimiento del servicio se hará cada vez más corto para mantener la rentabilidad del servicio [7].

Hasta ahora, la duración de las conexiones no se había tenido en cuenta como una información relevante para el enrutamiento, debido a que puede no conocerse de antemano. Si miramos los mercados de alquiler de ancho de banda [8] encontraremos que los clientes alquilan grandes cantidades de ancho de banda pero durante un periodo de tiempo limitado, por ejemplo, un año. En realidad, existen nuevas aplicaciones necesitan una enorme cantidad de ancho de banda entre dos localizaciones durante un periodo de tiempo. Ejemplos de este tipo de aplicaciones son HDTV, Grid Computing, Tele-inmersión, transferencia masiva de datos para almacenamiento o backup, etc.

Por lo tanto, es razonable esperar que los operadores de red puedan estimar de antemano la duración de las conexiones en las redes de transporte ópticas, principalmente en base a acuerdos de nivel de servicio o contratos con los clientes [5]. Existen trabajos previos en la literatura que han estudiado la protección de red en base al conocimiento de la duración de las conexiones (véase [9] por ejemplo).

Las conexiones conmutadas son más sensibles a los fallos en la red que las conexiones permanentes o las soft-permanentes, debido a que las conexiones conmutadas se solicitan cuando realmente se necesitan y requieren, a menudo, del nivel de disponibilidad más elevado. En un escenario de enrutamiento dinámico, es necesario actualizar las tablas de enrutamiento de forma periódica, para evitar situaciones de congestión y de fallos en la solicitud de nuevos lightpaths, permitiendo que el enrutamiento dinámico, basado en técnicas de ingeniería de tráfico, encuentre la mejor ruta en la red. En una red ASON/GMPLS, esta información puede ser distribuida mediante OSPF TE LSAs [10].

En el presente artículo, estudiaremos la influencia de la duración de las conexiones sobre la disponibilidad de la red, definiendo dos rangos de duración diferentes separados por una duración umbral (*Threshold Holding Time*, THT). Propondremos un nuevo algoritmo de enrutamiento diverso, que denominaremos FAR, para mejorar la disponibilidad de la red cuando la duración de las conexiones no sobrepasan el THT. El algoritmo propuesto será comparado con otros dos algoritmos de enrutamiento diverso basados en un algoritmo general. Los diferentes algoritmos difieren en si la información de fallos en la red se tiene en cuenta o no para el enrutamiento diverso. El comportamiento de los algoritmos será evaluado en cuanto a la probabilidad de bloqueo y a la disponibilidad.

Para comparar el comportamiento, se utilizarán dos diferentes topologías de red. La diferencia entre las topologías se encuentra principalmente en la media de grado nodal de la red y, por lo tanto, en su grado de mallado. Estas topologías han sido escogidas del estudio presentado en [11] para la Red de Transporte Óptica pan-Europea.

El resto del artículo está organizado de la siguiente manera: La sección 2 proporciona una introducción al cálculo de la disponibilidad en régimen permanente. Se presentan las dos redes de referencia y se calcula la disponibilidad teórica de los lightpaths. La sección 3 proporciona el conocimiento previo necesario sobre la protección de segmentos y sobre la influencia de la información de fallos sobre el enrutamiento diverso. Aquí se describen en detalle los diferentes algoritmos. En la sección 4 se describe el escenario de simulación. En la sección 5 se presenta la evaluación del comportamiento de las diferentes estrategias. La sección 6 presenta las conclusiones.

2. Disponibilidad

2.1. Disponibilidad en régimen permanente

Un aspecto importante cuando se tratan de comparar diferentes estrategias de enrutamiento en redes ópticas, es la disponibilidad. En general, la disponibilidad es la probabilidad de que un sistema se encuentre en operación en cualquier instante aleatorio futuro. La disponibilidad en régimen permanente puede expresarse como:

$$A = \frac{\text{UpTime}}{\text{UpTime} + \text{DownTime}} \equiv \frac{\text{MTTF}}{\text{MTTF} + \text{MTTR}}, \quad (1)$$

donde:

- *MTTR*: Tiempo medio de reparación, el tiempo esperado necesario para reparar el elemento.
- *MTTF*: Tiempo medio hasta el fallo, el tiempo esperado en que se producirá el siguiente fallo en el elemento, seguido de su reparación. MTTF se expresa habitualmente en FITs, el número de fallos en 10^9 horas.

Una medida relacionada es la indisponibilidad *U*, el complemento de la disponibilidad *A*:

$$U = 1\text{-}A \quad (2)$$

Si un sistema está formado por n componentes (o subsistemas) en serie, entonces todos los elementos deben estar operativos para que el sistema en su conjunto esté disponibles. Para elementos en serie, la disponibilidad del sistema completo es:

$$As = \prod_i A_i \quad (3)$$

Si MTTR es mucho mayor que MTTF:

$$As = \prod_i A_i \approx 1 - \sum_i U_i \quad [12] \quad (4)$$

Para elementos en paralelo, la disponibilidad del sistema completo es

$$Us = \prod_i U_i \quad (5)$$

En el presente artículo asumiremos los valores presentados en la Tabla 1 para MTTF y MTTR [13].

TABLA 1 VALORES TÍPICOS DE MTTF Y MTTR

Tasa de fallos de un transmisor	10,867 FITs
Tasa de fallos de un receptor	4,311 FITs

MTTR de una tarjeta de equipo	2 horas
MTTR de un cable de fibra óptica	12 horas
Tasa de fallos de un cable de fibra óptica	311 FITs/Km

Como se observa, el componente con una mayor tasa de fallos es el cable de fibra óptica y por lo tanto, la disponibilidad de un lightpath que utiliza recursos de un conjunto de enlaces y que no incorpora ningún mecanismo protección, puede ser calculado con suficiente precisión, por:

$$Apath \cong 1 - \sum_{i} U_{link}^{p}(i), \qquad (6)$$

donde $U_{link}^{p}(i)$ es la indisponibilidad del *i*-ésimo en el lightpath.

Por este motivo, en el presente artículo nos centraremos en el análisis de fallos de cables. De cualquier forma, el resultado que de aquí se derive puede ser adaptado al análisis de fallos de equipos.

2.2. Redes de referencia

En nuestros experimentos, hemos investigado el comportamiento de las diferentes estrategias de enrutamiento sobre dos topologías de red diferentes. Estas dos topologías han sido escogidas en base al estudio presentado en [11] sobre una red de transporte óptica pan-Europea, que las evalúa en términos del coste del diseño de red y de la disponibilidad de las conexiones, para diferentes tipos de tráfico. Ambas topologías conectan las mismas grandes ciudades europeas, tal y como se muestra en la Fig.1.

La topología denominada topología en anillo (*Ring Topology*, RT) es una topología poco mallada, mientras que la denominada topología triangular (*Triangular Topology*, TT) es altamente mallada, de hecho está formada por pequeños triángulos.

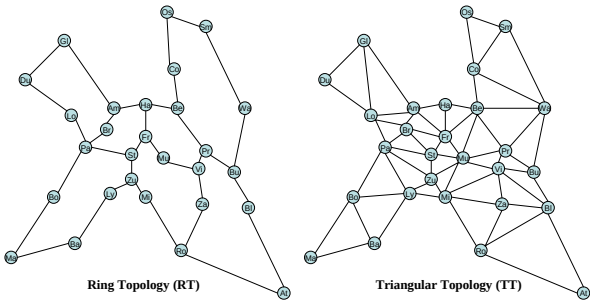

Figura 1 Topologías de Red

En la Tabla 2 se resumen algunos datos básicos de las dos topologías de red. Para obtener la longitud de las fibras que conectan los nodos en cada topología, se ha calculado la distancia aérea D entre cada par de nodos mediante la fórmula Haversine [14], que toma como entradas las coordenadas de latitud y la longitud de las dos localizaciones. La relación entre la longitud de la fibra L y la distancia aérea puede encontrarse en [15].

TABLA 2 DATOS BÁSICOS DE LAS TOPOLOGÍAS

	Núm. nodos	Núm. enlaces	Grado medio de los nodos	Distancia media de las fibras L (km)
RT	28	34	2.43	630
TT	28	61	4.36	638

Para apreciar la influencia de la topología seleccionada sobre la disponibilidad de los lightpaths, calcularemos algunos resultados numéricos. En la Tabla 3 se muestra el número medio de enlaces utilizados por los lightpaths establecidos sobre cada topología, donde Ruta A y Ruta B son las dos rutas disjuntas de una lightpath protegido 1+1. Estos valores se obtienen como resultado de simulación, y son básicamente idénticos para cualquiera de los diferentes algoritmos de enrutamiento presentados en este artículo. Con este dato, la disponibilidad teórica de los lightpaths, sin considerar su duración, puede ser calculado utilizando los valores de MTTF y MTTR, presentados en la Tabla 1 y aplicando las ecuaciones 1, 2, 5 y 6.

TABLA 3 DISPONIBILIDAD ESPERADA DE LOS LIGHTPATH

	Núm. Medio enlaces (ruta A)	Núm. Medio enlaces (ruta B)	Disponibilidad teórica de los lightpaths
RT	4.8	7.7	99.980%
TT	3.7	4.55	99.991%

3. Enrutamiento Diverso Consciente de los Fallos

3.1. Protección extremo a extremo y protección por segmentos

Para que una red pueda proporcionar protección de camino debe estar basada en un grafo biconexo [16], donde existen, al menos, dos rutas disjuntas de nodo entre cada par de nodos. En este tipo de redes, un lightpath protegido 1+1 consiste en dos rutas totalmente disjuntas entre los nodos origen y destino (protección extremo a extremo).

Para encontrar la pareja de caminos disjuntos de enlace de coste mínimo (o más corta) utilizamos el algoritmo la pareja de caminos disjuntos más cortos (*Shortest Disjoint Path Pair)*, que a su vez utiliza el algoritmo de Dijkstra modificado [17], para encontrar los caminos más cortos en grafos con uno o más enlaces con peso negativo pero sin bucles de peso negativo. Los enlaces de peso negativo aparecen en pasos intermedios del algoritmo de la pareja de caminos disjuntos más cortos.

Para ilustrar el algoritmo de la pareja de caminos disjuntos más cortos, haremos uso de la bien conocida topología "trap" (trampa) [18] que se muestra en la Fig.2a. En la topología *trap*, la ruta de trabajo puede bloquear todas las posibles rutas de protección disjuntas, aunque la topología sea biconexa. Por ejemplo, si intentamos encontrar la pareja de caminos más cortos, podríamos buscar el camino más corto (*p1*) desde el nodo 1 al 4,

resultando en el camino que muestra la Fig.2b. En este caso, no seremos capaces de encontrar ninguna otra ruta disjunta de enlace. De acuerdo con [19] las topologías *trap* pueden encontrarse en las redes de transporte de los operadores.

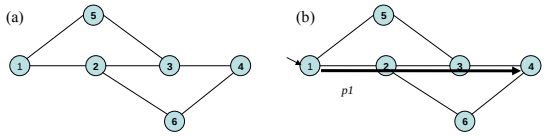

Figura 2 Topología Trap

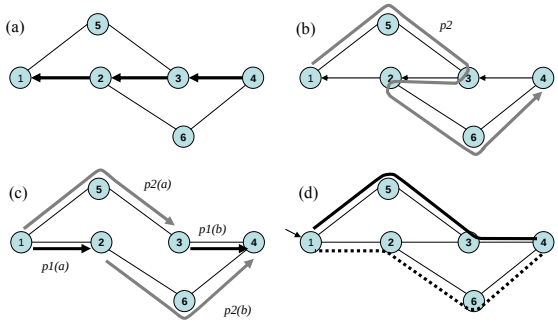

Figura 3 Algoritmo del par de caminos disjuntos más cortos

Los pasos del algoritmo, son:

- Buscar la ruta más corta desde 1 hasta 4: *p1* (Fig.2b).
- Crear los enlaces utilizados por *p1* como negativos inversamente dirigidos (Fig.3a).
- Buscar la ruta más corta en el grafo a): *p2* (Fig.3b).
- Eliminar los enlaces utilizados simultáneamente por *p1* y por *p2*; crear los segmentos *p1(a)*, *p1(b)* y *p2(a)*, *p2(b)* (Fig.3c).
- Alternar entre los segmentos para construir el par de caminos disjuntos (Fig.3d).

Algunas veces, bien porque la red no esté completamente desplegada en un área o la utilización de algunos enlaces de la red sea muy elevada o haya enlaces con fallo, no es posible encontrar una pareja de caminos totalmente disjunta. En estos casos, la opción que proporciona la mayor protección es proteger donde sea posible, es decir proteger por segmentos [20]. La Fig.4 muestra ambos conceptos. Hay que tener en cuenta que en la protección por segmentos hay nodos adicionales, además de los nodos extremos, que realizar la función de conmutación de protección (nodos B2 y B3 en la Fig.4b).

Para implementar la protección por segmentos, el grafo que representa la red debe ser descompuesto en sus *componentes biconexas*, localizando los nodos cuyo simple fallo podría partir el grafo en dos subgrafos separados. Estos nodos se denominan *puntos de articulación* (Fig. 5).

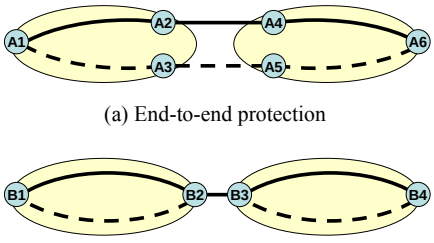

Figura 4 Protección extremo a extremo y por segmentos

Para encontrar todas las componentes biconexas de un grafo, utilizamos un procedimiento basado en recorrer el grafo primero en profundidad, seguido de una fase de *backtracking*. La descripción del procedimiento puede encontrarse en [16].

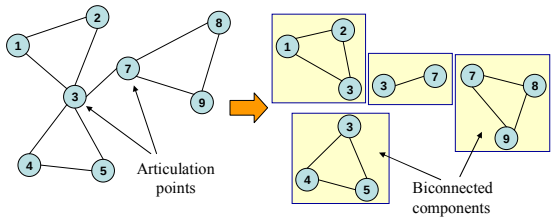

Figura 5 Descomposición del grafo de red

Para encontrar la pareja de caminos más cortos entre do nodos, se crea una vista de la red localizando las componentes biconexas. Para cada componente biconexa se crea un nuevo árbol de caminos más cortos siguiendo el criterio de mínimo número de saltos, ejecutando el algoritmo de Dijkstra Modificado. Para calcular las dos rutas disjuntas de un path, se utiliza el algoritmo de la pareja de caminos disjuntos más cortos (*Shortest Disjoint Path Pair Algorithm*) en cada una de las componentes biconexas. Conectando los segmentos, se obtiene la pareja de caminos disjuntos por segmentos.

3.2. Influencia de la información de fallos sobre el enrutamiento diverso

En un escenario de red dinámico, el cálculo de los lightpaths protegidos debe de tener en cuenta el estado global de la red, para conocer qué recursos están disponibles para ser utilizados. Además de la disponibilidad de los recursos de red (recursos que no están siendo utilizados por otro lightpath en la red), proponemos tener en cuenta también su estado de fallo.

La Fig. 6a muestra una red con un fallo en el enlace entre los nodos 2 y 3. Supongamos que llega una petición al nodo 1 para establecer un lightpath protegido hacia el nodo 4. Una opción, en la fase de enrutamiento, es la de escoger las rutas sin tener en cuenta los fallos en la res (el fallo en el enlace entre el nodo 2 y 3 no se tiene en cuenta). Denominados a esta estrategia, algoritmo de Enrutamiento Independiente de los Fallos (*Failure Independent Routing*, FIR) (Fig. 6b). En esta opción, si el enlace con fallo se repara y posteriormente falla el enlace que conecta los nodos 4 y 5, el lightpath protegido continuará en funcionamiento.

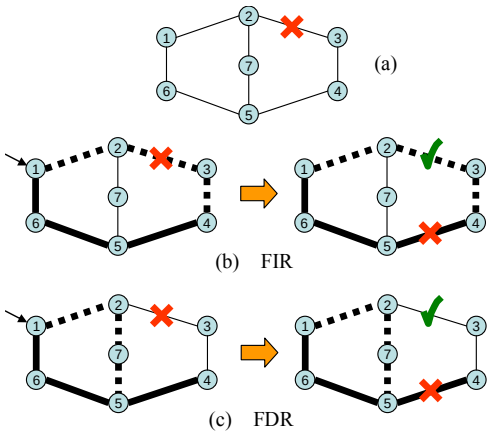

Figura 6 Influencia de la información de fallos en el enrutamiento diverso

En este artículo definiremos el algoritmo de Enrutamiento Dirigido por los Fallos (*Failure Driven Routing*, FDR) (Fig. 6c). Este algoritmo de enrutamiento tiene en cuenta los fallos en la red en el momento en que llega la petición de conexión. Si el enlace en fallo es reparado, pero el enlace que conecta los nodos 4 y 5 falla, el lightpath protegido estará indisponible con un solo recurso con fallo.

Si la duración del lightpath protegido es muy corta, la probabilidad de que se vea afectado por dos fallos consecutivos es muy pequeña, por lo que tener en cuenta la información sobre los fallos garantiza que el lightpath esté disponible cuando sea establecido. Por otra parte, si la duración del lightpath es muy larga, la probabilidad de que se vea afectado por dos fallos consecutivos es muy alta. Sin embargo, los lightpaths no tienen garantía de estar disponibles en el momento del establecimiento.

De esta forma hemos introducido cómo la duración de las conexiones tiene un efecto directo sobre la disponibilidad del lightpath y de su relación con los valores de MTTF y MTTR.

La tercera opción de enrutamiento diverso que vamos a considerar es el algoritmo que denominamos Enrutamiento Consciente de los Fallos (*Failure Aware Routing*, FAR). El algoritmo de enrutamiento tiene en cuenta los fallos en la red en el momento en que llega la petición y fuerza que la ruta de trabajo utilice enlaces sin fallos, pero permite que la ruta de protección utilice enlaces con fallo. De esta forma, todos los lightpaths tienen garantía de estar disponibles en el momento en que se establecen y permite que la ruta más corta sea elegida aunque esté afectada por algún fallo, en espera de que sea reparada. De esta forma, la estrategia de enrutamiento FAR selecciona una mejor pareja de rutas que las estrategias FIR y FDR.

Por otra parte, la estrategia FIR utilizará los mismos recursos independientemente de los fallos en la red, ya que la información de los fallos no es considerada por el algoritmo. Sin embargo, la estrategia FDR puede utilizar más recursos que la estrategia FIR, buscando una ruta sin enlaces con fallo, o menos recursos que la estrategia FIR, si no se encuentra una ruta disjunta, tal y como explicaremos en el siguiente ejemplo.

En la Fig. 7 hay tres rutas disjuntas disponibles entre un nodo origen y otro destino. La ruta 2 usa más recursos que la ruta 1 pero menos recursos que la ruta 3. Con el tiempo, las rutas se verán afectadas por fallos. En este escenario, dependiendo del momento en que se solicita el establecimiento del lightpath protegido (ta,..,tg), las estrategias de enrutamiento diverso FIR, FDR y FAR seleccionarán rutas diferentes.

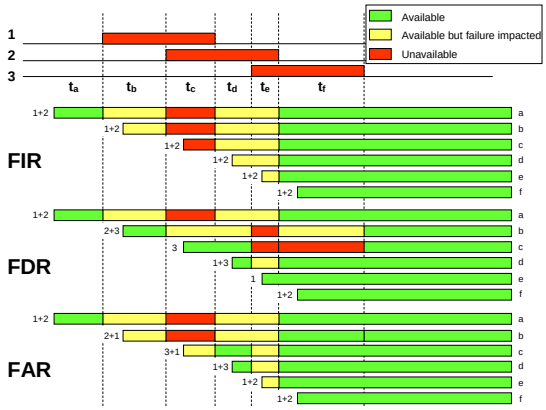

Figura 7 Comportamiento de las estrategias en enrutamiento con los fallos

- Las peticiones entrantes en t_a y en t_f darán como resultado las mismas rutas utilizando cualquiera de las diferentes estrategias (lightpaths *a* y *f*). Las rutas seleccionadas son la 1 y la 2 ya que ambas están libres de fallo y son las que utilizan menos recursos. De hecho la estrategia FIR siempre usará las rutas 1 y 2.
- Las peticiones entrantes en t_b usarán diferentes rutas dependiendo de la estrategia utilizada. La estrategia FDR seleccionará las rutas 2 y 3 y la estrategia FAR seleccionará las rutas 2 y 1. Comparando el resultado de las tres estrategias, el lightpath creado con la estrategia FDR presenta el mismo periodo de indisponibilidad que los creados con las estrategias FIR y FAR, pero la indisponibilidad del primero se produce más tarde. Por lo tanto, los lightpaths de muy corta duración presentarán una disponibilidad más alta utilizando la estrategia FDR.
- Las peticiones entrantes en t_c utilizarán diferentes rutas dependiendo de la estrategia utilizada. La estrategia FDR utilizará únicamente la ruta 3, ya que es la única ruta libre de fallos en este momento, dando como resultado un lightpath no protegido. Por otra parte, el lightpath seleccionado por la estrategia FIR está indisponible en el momento en que se establece. En este caso, los resultados de las estrategias FIR y FDR puede mejorarse seleccionando las rutas 3 y 1, tal y como hace la estrategia FAR. Una situación similar aparece para las peticiones entrantes en t_e.

En el siguiente apartado se describirán en detalle las tres estrategias, FIR, FDR y FAR.

3.3. Algoritmos de enrutamiento

3.3.1. Enrutamiento Independiente de los Fallos (FIR)

El algoritmo de Enrutamiento Independiente de los Fallos (FIR) calcula las rutas del lightpath teniendo en cuanta únicamente la ocupación de los enlaces de la red. Cada vez que llega una petición de lightpath a un nodo, la estrategia FIR crea una vista de la red, localizando las componentes biconexas de la red. De esta forma, se elige la pareja de rutas más cortas para cada petición de lightpath, pero estas rutas pueden estar afectadas por fallos.

3.3.2. Enrutamiento Dirigido por los Fallos (FDR)

La diferencia con la estrategia explicada en el apartado anterior, es que la estrategia de Enrutamiento Dirigida por los Fallos incluye el estado de fallo de los enlaces para construir la vista de la red. De esta forma, las peticiones entrantes de lightpath serán enrutadas a través de enlaces libres de fallo.

3.3.3. Enrutamiento Consciente de los Fallos (FAR)

En esta estrategia, la ruta de trabajo es forzada a utilizar enlaces libres de fallo mientras que la ruta de protección se la permite utilizar enlaces con fallo. De esta forma, todos los lightpaths tienen garantía de estar disponibles en el momento en el que son establecidos y, además, se elige el camino más corto como ruta de protección para asegurar que se utiliza la mejor ruta cunado los fallos en la red sean reparados.

Para desarrollar esta estrategia, es importante revisar el algoritmo de Dijkstra Modificado para evitar bucles con coste neto negativo. Estos bucles pueden aparecer cuando se utiliza el algoritmo de la pareja de rutas disjuntas más cortas con un camino (*p1*) construido a partir de una vista de la red construida tenido en cuanta los fallos en la red, para obtener un camino (*p2*) desde una vista de la red construida sin tener en cuenta los fallos en la red. La modificación implementada primero chequea los nodos re-visitados para detectar un posible bucle con coste neto negativo. El listado 1 contiene el pesudocódigo del algoritmo FAR.

Listado 1 PSEUDOCÓDIGO DE FAR

```
Crear Vista de la red (Consciente de fallos)
Buscar ruta al destino (p1)
Crear Vista de la red (No consciente de fallos)
Para cada segmento en p1
    Buscar ruta disjunta en la componente
    biconexa
    Ruta disjunta extremo a extremo += ruta
    disjunta
```

4. Escenario de Simulación

Para comparar las diferentes estrategias de enrutamiento, hemos construido un simulador de propósito específico dirigido por eventos. El escenario de simulación consiste de una red sobre la que se van ejecutando los eventos.

En el modelo de simulación consideramos que cada nodo mantiene información sobre el estado global de la red para el enrutamiento y que esta información es actualizada periódicamente. En los siguientes apartados describiremos en detalle el escenario de simulación que adoptamos.

El simulador ha sido concebido para analizar la influencia de la duración de las conexiones sobre la disponibilidad de las conexiones conmutadas. De esta forma, consideraremos que la red solamente transporta este tipo de conexiones e inicialmente cada enlace dispone de 40 canales libres para ser utilizados por los lightpaths conmutados.

Sin embargo, en redes ASON reales, las conexiones permanentes, soft-permanentes y conmutadas han de coexistir simultáneamente. Mientras que las conexiones permanentes se proporcionan como líneas alquiladas y son establecidas por el sistema de gestión (NMS), tanto las soft-permanentes como las conmutadas requieren del soporte de un plano de control inteligente. De cualquier forma, la duración tanto de las conexiones permanentes como de las soft-permanentes puede considerarse infinito y, por lo tanto, no ejercen ninguna influencia sobre los resultados mostrados en el presente artículo, excepto la de reducir la capacidad disponible para las conexiones conmutadas.

4.1. Modelo de Tráfico

Mientras que el tráfico telefónico (de voz) se intercambia, principalmente, entre localizaciones geográficamente cercanas, el intercambio de tráfico de Internet está mucho menos relacionado con la distancia.

En nuestro sistema de simulación, el tráfico se modela utilizando la aproximación de Dwivedi y Wagner [21]. Este modelo diferencia entre tres tipos de tráfico: tráfico de voz, tráfico de datos de transacciones (tráfico IP de negocios) y tráfico Internet (tráfico IP no relacionado con negocios). El tráfico total resultante entre dos localizaciones A y Z se obtiene de la suma de los patrones anteriores.

De acuerdo con [11] el tráfico telefónico es inversamente proporcional a la distancia entre el origen y el destino ($D_{A\text{-}Z}$), el tráfico de transacciones es inversamente proporcional a la raíz cuadrada de la distancia y el tráfico de Internet es independiente de la distancia.

$$Telefónico_{A\text{-}Z} = \frac{C_v}{D_{A-Z}} \qquad (7)$$

$$Transacciones_{A\text{-}Z} = \frac{C_t}{D_{A-Z}^{1/2}} \qquad (8)$$

$$Internet_{A\text{-}Z} = C_i \qquad (9)$$

Las constantes C_v, C_t y C_i, incluyen parámetros como la población, el número de empleados de empresas no relacionadas con la producción, el número de

servidores de Internet y una estimación del crecimiento del tráfico.

En este artículo asumiremos una mezcla de tráfico de las peticiones que llegan a cada nodo con un 40% de tráfico telefónico, un 25% de tráfico de transacciones y un 35% de tráfico de Internet. Todas las peticiones son de lightpaths protegidos.

Para calcular el destino de una petición de conexión que llega a un nodo fuente, se generan dos números aleatorios. El primero define el tipo de tráfico y el segundo se aplica sobre un *array* ordenado que contiene la lista de todos los nodos de la topología de red, para obtener el nodo destino. El *array* se ordena de acuerdo con el tipo de tráfico seleccionado en el primer paso, utilizando las ecuaciones (7-9).

4.2. Eventos

Se han considerado cuatro tipos de eventos en la simulación, son los siguientes:

- *Petición de establecimiento de Lightpath*: Dada una demanda (nodo fuente, nodo destino, duración del lightpath, lightpath protegido/no protegido), trata de establecer (determinar la ruta y reservar los recursos) un nuevo lightpath en la red, teniendo en cuenta la ocupación actual de los enlaces (y su estado de fallo si es el caso). Si lo consigue, programa el evento de liberación del lightpath.
- *Liberación de Lightpath*: Libera los recursos utilizados por el lightpath.
- *Corte de Cable*: Pone el enlace en estado de fallo y programa un evento de reparación del cable.
- *Reparación de Cable*: Pone el enlace en estado de no fallo.

4.3. Procesos Estocásticos

La simulación consiste en la sima de dos familias de procesos estocásticos independientes [22]:

- *Peticiones de Conexión*: Las peticiones de conexión llegan a cada nodo de forma independiente, de acuerdo con un proceso de *Poisson* con un tiempo medio entre llegadas predefinido (*iat*). La duración de las conexiones está exponencialmente distribuida, con una duración media predefinida (*ht*). El destino de cada conexión está definido por la mezcla de los patrones de tráfico descritos previamente en el apartado de *Modelo de Tráfico*. La intensidad de tráfico media en Erlangs, que sale de cada nodo, es por tanto:

$$E=ht/iat \qquad (10)$$

- *Cortes de Cable*: Los cortes de cable aparecen en cada enlace de la red de forma independiente de acuerdo a un proceso de *Poisson*, con un tiempo medio entre fallos (MTTF) predefinido, y dependiendo de la longitud del enlace. Para calcular el tiempo de reparación de los fallos, utilizamos una distribución *Weibull* con un parámetro de forma $\alpha=2$ y un tiempo medio de reparación (MTTR) predefinido.

4.4. Contadores estadísticos

Durante la ejecución de la simulación, al final de cada evento se actualizan los siguientes contadores estadísticos. Los principales contadores, son:

- *Número de peticiones de Lightpaths (RPn):* Este contador se incrementa después de cada llegada de un evento de petición de establecimiento de lightpath.
- *Número de Lightpaths creados (Pn):* Este contador se incrementa después de la ejecución satisfactoria de un evento de establecimiento de lightpath.
- *Número de cortes de enlace (Cn)*: Este contador se incrementa después de la ejecución de un evento de corte de cable.
- *Número de enlaces reparados:* Este contador se incrementa después de la ejecución de un evento de reparación de cable.
- *Número de lightpaths, $P(t_i)$:* El número de lightpaths en la red en el instante *t*.
- *Número de lightpaths indisponibles, $U(t_i)$:* El número de lightpaths indisponibles en la red en el instante *t*.

4.5. Medidas estadísticas

Después de la ejecución de la simulación, se calcula un conjunto de medidas. Las más importantes, son:

- Tráfico Total (disponible + indisponible): Minutos de tráfico.

$$\mathrm{Tt(n)} = \int_0^{T(n)} P(t)dt \qquad (11)$$

- Tráfico indisponible: Minutos de tráfico indisponible.

$$Ut(n) = \int_0^{T(n)} U(t)dt \qquad (12)$$

- Disponibilidad:

$$A = 1 - \frac{Ut(n)}{Tt(n)} \qquad (13)$$

- Probabilidad de bloqueo:

$$B = \frac{\mathrm{RPn - Pn}}{RPn} \qquad (14)$$

5. Evaluación del rendimiento

Los resultados presentados a continuación son el promedio de 10 ejecuciones de la simulación. Cada ejecución termina cuando se han ejecutado más de 200.000 eventos de establecimiento de conexión y se más de 20.000 cortes de cable.

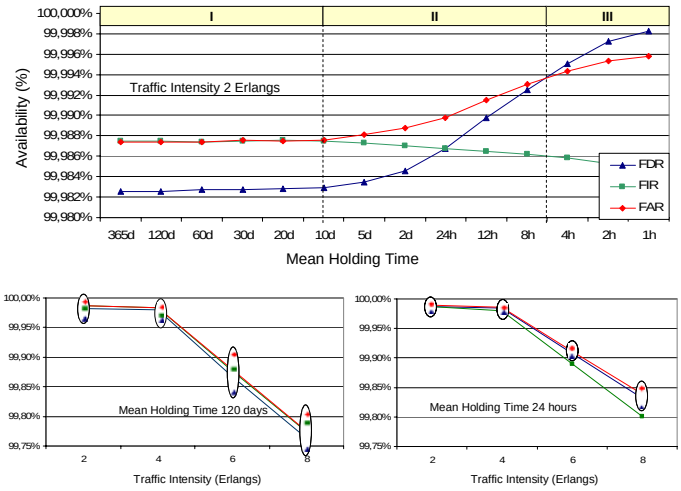

Figura 8 Disponibilidad en RT

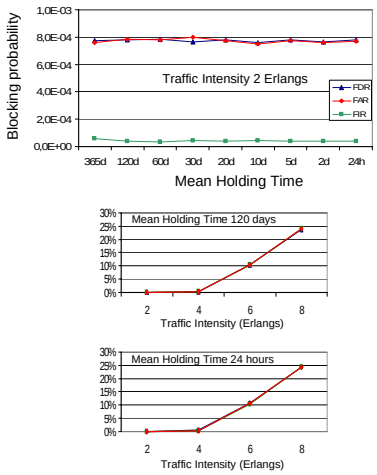

Figura 9 Probabilidad de bloqueo en RT

La parte superior de la Fig. 8 muestra la disponibilidad de la red de las estrategias de enrutamiento sobre la topología en anillos, RT. La gráfica representa la disponibilidad como función de la duración de los lightpaths, para una intensidad de tráfico de 2 Erlangs. Para ilustrar los efectos opuestos explicados anteriormente, hemos dividido la gráfica en tres zonas.

Para duraciones de conexión largas (>20*MTTR; Zona I) no tener en cuenta los fallos en la red para el enrutamiento (estrategia FIR) resulta en una mejor disponibilidad, ya el algoritmo encuentra la mejor pareja de rutas disjuntas. Sin embargo, para duraciones de conexión cortas (20*MTTR ≥ duración media ≥ MTTR; Zona II) eliminar los recursos con fallo para el enrutamiento (estrategia FDR) resulta en una disponibilidad mucho mayor, ya que los lightpaths tienen garantía de estar disponibles en el momento en que se establecen. Como explicamos anteriormente, la estrategia FAR, al ser una mezcla entre las dos anteriores, proporciona la mejor disponibilidad tanto para largas como para cortas duraciones de conexión.

Utilizando esta gráfica, estimamos el valor de la duración umbral THT en 12 horas, esto es, el MTTR. Para duraciones de conexión muy cortas (<MTTR; Zona III) el efecto de fallos simultáneos es mayor que el de fallos consecutivos. De esta forma, buscando rutas de trabajo y de protección sin utilizar enlaces con fallo hace que la estrategia FDR sea la mejor.

Las gráficas de la parte inferior de la Fig. 8 refuerzan esta conclusión. Éstas representan la evolución de la disponibilidad con la intensidad de tráfico para lightpaths de duración media 120 días y 24 horas. Para apreciar las posiciones relativas se ha realizado un *zoom*. Como se muestra, las estrategias mantienen sus posiciones relativas.

La Fig. 9 muestra la evolución de la probabilidad de bloqueo para las estrategias de enrutamiento, obtenida sobre la poco mallada topología en anillos.

La gráfica de la parte superior representa la evolución de la probabilidad de bloqueo en función de la duración media de los lightpaths para una intensidad de tráfico de 2 Erlangs.

Como puede observarse, la probabilidad de bloqueo permanece en el mismo nivel para las estrategias FDR y FAR y presenta un valor levemente superior respecto de la estrategia FIR. Este efecto es debido al hecho de que las primeras estrategias buscan primero una ruta libre de fallos y si no la encuentran fallan, resultando en una mayor probabilidad de bloqueo. La estrategia FIR presenta una probabilidad de bloqueo cercano al 0%, debido a que hay suficientes recursos libres en la red, aunque algunos de ellos estén afectados por un fallo. Por lo tanto, la diferencia de probabilidades de bloqueo se transforma en una mejor disponibilidad.

La Fig. 11 muestra la disponibilidad de la red para las tres estrategias de enrutamiento sobre la altamente mallada topología triangular (TT). Aquí pueden apreciarse efectos similares a los anteriores.

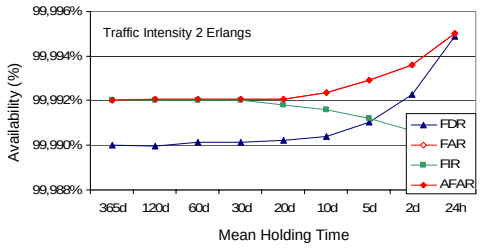

Figura 10 Disponibilidad en TT

Respecto de la probabilidad de bloqueo, todas las estrategias presentan valores similares, sobre la topología triangular, a los presentados para la topología en anillos, RT.

Conclusiones

En el presente artículo hemos presentado la influencia de la información de los fallos sobre el enrutamiento diverso. Además, hemos introducido un algoritmo de enrutamiento diverso que mejora la disponibilidad de las conexiones bajo demanda y hemos definido la duración umbral THT. Se han evaluado tres estrategias mediante simulación.

Para una duración larga de las conexiones (por ejemplo, del orden de días) la estrategia FIR proporciona la mejor disponibilidad, ya que el algoritmo de enrutamiento diverso encuentra el mejor par de rutas disjuntas. Por otra parte, cuando las conexiones tienen una duración muy corta, utilizando la estrategia (FDR) da como resultado una disponibilidad mucho mayor, ya que los lightpaths se crean garantizando que las rutas no tienen ningún fallo cuando son establecidas. Finalmente, la estrategia FAR (la ruta de trabajo utiliza recursos sin fallo, mientras que la de protección puede utilizar recursos con fallo), al ser una especie de mexcal entre las estrategias FIR y FDR, proporciona la mejor disponibilidad para duración de las conexiones largas y cortas.

Mediante simulación, hemos encontrado que el valor de THT es de 12 horas, es decir, el valor del MTTR empleado.

Respecto de la probabilidad de bloqueo, las tres estrategias presentan básicamente los mismos valores, aunque las estrategias FDR y FAR presentan una probabilidad de bloqueo ligeramente mayores que la estrategia FIR. Esto es debido al hecho de que las dos primeras estrategias buscan una ruta sin fallos y si no la encuentran todos fallan. Sin embargo, la estrategia FIR, al no tener en cuenta los fallos en la red, creará el path aunque éste se encuentre en fallo en el momento del establecimiento.

De acuerdo con estos resultados, proponemos el uso general de la estrategia FAR para el enrutamiento bajo demanda de lightpaths con mecanismo de protección dedicado 1+1 cuando la duración de las conexiones sea inferior a 12 horas.

Agradecimientos

Este trabajo ha sido soportado parcialmente por el proyecto RINGING (TEC2005-08051-C03-02) del MEC.

Referencias

[1] ITU-T Rec. G.8080/Y.1304, “Architecture for the Automatically Switched Optical Networks”, Nov. 2001, and Am. 1, Mar. 2003.

[2] E. Mannie, “Generalized Multi-Protocol Label Switching (GMPLS) Architecture” RFC-3945, Oct. 2004.

[3] Optical Internetworking Forum, “User Network Interface (UNI) 1.0 Signaling Specification, Release 2”, Feb. 2004

[4] A. Jajszczyk, “Automatically Switched Optical Networks: Benefits and Requirements”, IEEE Optical Communications, Feb. 2005.

[5] J-P. Vasseur, M. Pickavet, P. Demeester, “Network Recovery - Protection and Restoration of Optical, SONET-SDH, IP and MPLS”, Elsevier, 2004.

[6] R. Appelman, Z. Zalevsky, “All-Optical Switching Tecnologies for Protection Applcations”, IEEE Optical Communications, Nov. 2004.

[7] A. Iselt, A.Kirstdter and R. Chahine, “The role of ASON and GMPLS for the bandwidth trading market”. In Proc. 1st International Conference on E-business and Telecommunications Networks (ICETE2004), Aug. 2004.

[8] http://www.fiberloops.com

[9] M. Tornatore, C. Ou, J. Zhang, A. Pattavina and B. Mukherjee, “PHOTO: an efficient shared-path protection strategy based on connection-holding-time awareness”. In IEEE\OSA Journal on Lightwave Technology, Vol. 23, No. 10, pp 3138-3146, Oct 2005.

[10] K. Kompella, Y. Rekhter, “OSPF Extensions in Support of Generalized Multi-Protocol Label Switching (GMPLS)”, RFC 4203, Oct. 2005.

[11] S. De Maesschalck, et. al, “Pan-European Optical Transport Networks: An Availability-based Comparison”, Photonic Networks Communications, vol.3 no.5 May 2003, pp. 203-225.

[12] R. L. Freeman, “Telecommunications System Engineering”, 3rd Ed. Wiley, 1996, pp. 444-447.

[13] M. To, P. Neusy, “Unavailability Analysis of Long-Haul Networks”, IEEE J. on Sel. Areas in Comm. Vol.12, no 1, Jan. 1994, pp. 100-109.

[14] “Calculate distance and bearing between two Latitude/Longitude points”, http://www.movable-type.co.uk/scripts/LatLong.html.

[15] ETSI Rec. EN 300 416 “Network Aspects (NA); Availability performance of path elements of international digital paths” v. 1.2.1, August 1998

[16] W. D. Grover, “Mesh-Based Survivable Networks”, Prentice Hall PTR, 2004

[17] R. Bhandari, “Survivable Networks: Algorithms for Diverse Routing”, Kluwer Academic Publishers, 1999.

[18] D. Dunn, W. Grover, M. MacGregor, “Comparison of k-shortest paths and maximum flow routing for network facility restoration,” IEEE Journal on Selected Areas of Communications, vol. 2, no. 1, 1994, pp. 88–99.

[19] B. Doverspike, G. Li, and C. Kalmanek, “Fiber Span Protection in Mesh Optical Networks”, Opt. Net., May/June 2002.

[20] L. Berger, I. Bryskin, D. Papadimitriou, A. Farrel, “GMPLS Based Segment Recovery”, Internet Draft draft-ietf-ccamp-gmpls-segment-recovery-02.txt, May 2005.

[21] A. Dwivedi, R. Wagner, “Traffic Model for USA Long-Distance Optical Network”, Proc. of Optical Fiber Communication Conference (OFC) 2000 Vol.1, TuK1-1, pp. 156-158.

[22] A. Law, D. Kelton, “Simulation Modeling and Analysis” 3rd Ed, McGrawHill 2000