Proyecto de Grado

presentado el día de

Universidad de La República, UdelaR

para obtener el título de

INGENIERO EN COMPUTACIÓN

por

Daniel LENA MESSERE

Instituto de Computación - INCO

UNIVERSIDAD DE LA REPÚBLICA
FACULTAD DE INGENIERÍA

Titulo del Proyecto :

Confiabilidad de Redes con Fallas Hostiles

Comité examinador:

Dr. Ing. Franco	ROBLEDO	Tutor
Dr. Ing. Pablo	ROMERO	Tutor
Prof. Ing. Omar	VIERA	
Dr. Ing. Pedro	PIÑEYRO	
Dr. Ing. Libertad	TANSINI	

Índice general

RESUMEN

En una red en la que los enlaces se encuentran sujetos a fallas aleatorias e independientes la confiabilidad mide la probabilidad de que, dado un estado, un conjunto de nodos terminales distinguidos se mantenga conectado mediante enlaces operativos. Esta medida es considerada como de gran relevancia según el sistema (comunicaciónes, vial, etc) en concreto con el que se esté tratando y su tamaño. El mismo escenario donde no solo fallan las aristas sino los nodos no distinguidos por igual, es tratado a lo largo de este documento como el modelo hostil. Este trabajo se centra en el cálculo de la confiabilidad de redes bajo el modelo hostil. Tomaremos como hipótesis de trabajo la independencia de fallas de los componentes no terminales y los enlaces, mientras que consideraremos como perfecto el funcionamiento de sus terminales distinguidos. La red opera correctamente siempre que los terminales (nodos distinguidos de la misma) permanezcan comunicados a través de caminos que incluyan tanto aristas como nodos operativos. El problema de calcular la anticonfiabilidad bajo este modelo generaliza el problema clásico del mismo, y pertenece como consecuencia a la clase de problemas $\mathcal{NP}$-Difíciles.

En este documento se desarrollan y contrastan dos métodos estadísticos para el cálculo de la confiabilidad del modelo hostil, junto con el método de Monte Carlo que les da origen. El primer método se denomina Reducción de la Varianza Recursiva, o RVR, y ha demostrado ser exitoso desde sus orígenes para la estimación de la confiabilidad en el modelo clásico. El segundo método es conocido como Muestreo por Importancia, y es especialmente adecuado en contextos de redes altamente confiables donde el evento de falla de la red se torna poco probable. Para esto propone un cambio de medida óptimo donde los eventos raros se tornan más probables. Se realizan las modificaciones necesarias para su adaptación al modelo hostil y se contrastan luego los resultados al aplicarlos a ciertos grafos comunes al estudio de la confiabilidad de redes.

Palabras Clave: Confiabilidad de Redes; Modelo Hostil; Complejidad Computacional; Monte Carlo; Reducción de la Varianza Recursiva; Muestreo por Importancia.

Trabajos relacionados: Como producto de este proyecto se ha enviado un artículo a la conferencia CLAIO 2016 (Conferencia Latino Americana de Investigación Operativa) y ha sido aprobado para su publicación y presentación, a ser realizada entre el 2 y el 6 de octubre de 2016: Lena, D., Robledo, F., Romero, P. "Modelo Hostil de Redes con Fallas en Aristas y Nodos".

Parte I

Introducción

1

Introducción

1.1. Planteo del problema

El desarrollo de las redes de comunicación, la diversificación de los servicios y las numerosas funcionalidades, sumados a los factores de seguridad y calidad de los servicios que hoy en día es cada vez más necesario ofrecer, han orientado cada vez más los esfuerzos hacia el diseño de las redes, priorizando la disponibilidad del servicio. El estudio matemático de la confiabilidad clásica se basa en el modelo de grafos aleatorios con fallas independientes [**?**]. Rosenthal ha demostrado que el cálculo de la confiabilidad en el problema tradicional pertenece a la clase $\mathcal{NP}$-Difícil [**?**], y dado que este modelo es una simplificación del modelo hostil donde la probabilidad de operacion de los nodos es 1, es decir que son perfectos, podemos considerar que el modelo hostil también tiene complejidad $\mathcal{NP}$-Difícil.
En estos casos normalmente se recurre a aproximaciones basadas en la simulación de Monte Carlo [**?**]. En el contexto de redes altamente confiables los métodos tradicionales como el método de Monte Carlo Crudo no logran un buen desempeño en la estimación de la medida de confiabilidad [**?**]. Bajo este escenario, una alternativa válida es aplicar alguna de sus variantes las cuales se enfocan en la reducción de la varianza mejorando así la precisión de las estimaciones respecto al método original.

Este documento se organiza de la siguiente manera. En el Capítulo **??** se presenta una descripción del problema, y conceptos fundamentales de complejidad computacional. Se enmarcan los modelos de confiabilidad de redes en un modelo más abstracto y general de Sistemas Binarios Estocásticos. El Capítulo **??** resume antecedentes relativos a modelos de confiabilidad clásicos, indicando métodos exactos de tiempo exponencial y métodos basados en Monte Carlo (de tiempo polinomial) y se realiza una reseña de los mismos. Luego se presenta el análisis de los métodos, Reducción Recursiva de la Varianza (RVR por sus siglas en inglés) y de una instancia del método de Muestreo por Importancia (IS-AZVIS por sus siglas en inglés) aplicados al modelo hostil de arista-nodo confiabilidad, donde se asume que tanto los nodos no distinguidos como las aristas son factibles de fallas. Y se plantea el problema central de estudio de este trabajo: la estimación de la anticonfiabilidad de una red bajo estas hipótesis. Luego en el Capítulo **??** se realiza la presentación y análisis de los resultados al aplicar dichos algoritmos a una serie de grafos comunes en la literatura y a algunos ejemplos de redes reales.

1.2. Complejidad computacional

Un problema es una pregunta que espera una respuesta, y está relacionado a cierta cantidad de parámetros que al instanciarlos determinan una entrada particular del problema. Un algoritmo es un conjunto finito de pasos que resuelve toda instancia de un problema. Cuando nos enfrentamos a un problema, la intención es la de encontrar un algoritmo que lo resuelva, es decir, que resuelva toda instancia del mismo. La teoría de la complejidad computacional nos permite identificar clases bajo las cuales son agrupados problemas equivalentes. En general la eficiencia de un algoritmo dado para un problema determinado, se mide en función de la cantidad de operaciones necesarias para resolver dicho problema.

Los fundamentos de la teoría de la decisión fueron introducidos por Stephen Cook en 1971 en su artículo [**?**] y complementado luego por Richard Karp [**?**]. Inicialmente se consideran dos clases de problemas: la clase $\mathcal{P}$ correspondiente a los problemas que pueden ser resueltos por algoritmos de tiempo polinomial respecto al tamaño de la instancia de entrada por una máquina determinista, y la clase $\mathcal{NP}$ cuyos problemas pueden ser resueltos por algoritmos de orden polinomial utilizando máquinas no-deterministas. Dado que cualquier problema que puede ser resuelto por un algoritmo en tiempo polinomial ($\mathcal{P}$) por una máquina determinista también puede ser resuelto por un algoritmo polinomial por máquinas no deterministas, sabemos que $\mathcal{P} \subseteq \mathcal{NP}$. Aún no se ha podido demostrar que exista un problema que pertenezca a $\mathcal{NP}$ y que a su vez no pertenezca a $\mathcal{P}$, pero hay un gran conjunto de problemas que son candidatos a no poder ser resueltos en orden polinomial y por lo tanto a estar incluídos en $\mathcal{NP}$ y excluídos de $\mathcal{P}$. Este es un problema abierto que permanece en el corazón de la Teoría de la Computación.

La técnica principal utilizada para demostrar que dos problemas pertenecen a la misma clase es la de reducir uno a partir del otro, facilitando una transformación que mapee cualquier instancia del primer problema en un instancia equivalente de la segunda. Esta transformación proporciona los medios para convertir cualquier algoritmo que resuelva el segundo problema en un algoritmo correspondiente para resolver el primer problema [**?**].

Por lo tanto, un problema que pertenece a la clase $\mathcal{NP}$ puede ser reducido a otro problema perteneciente a la clase $\mathcal{NP}$ si existe algún algoritmo polinomial que sea capaz de transformar cada instancia del problema original en una instancia del nuevo problema. De forma análoga, si tenemos dicha transformación polinómica de instancias entre un problema y otro garantizaremos que cualquier algoritmo de tiempo polinomial que resuelva el segundo problema se pueda transformar en un algoritmo que resuelva el primer problema también en tiempo polinomial.

Luego, dentro de los problemas que se encuentran en $\mathcal{NP}$ se distinguen una gran cantidad de ellos que han sido identificados y catalogados como los más difíciles de la clase. Estos problemas comparten una equivalencia en su dificultad de resolución por no conocerse un algoritmo que proporcione una solución en tiempo polinomial respecto a la entrada. A esta característica se la conoce por el término intratabilidad, y refiere a aquellos problemas para los cuales no existe un algoritmo eficiente que los resuelva, lo mismo decir que no se conoce un algoritmo que los resuelva en tiempo polinomial respecto al tamaño de la instancia de entrada. A esta categoría se la conoce como la categoría de los problemas $\mathcal{NP}$-Completos. Todos estos conceptos esenciales de la teoría de la computación fueron presentados por Cook, quien además probó que todo problema perteneciente a la clase $\mathcal{NP}$ admite una reducción polinomial a un problema es-

pecial, el problema de decisión de satisfactibilidad booleana SATISFACTIBILIDAD: dada una proposición lógica en su forma normal conjuntiva, determinar si existe una asignación de verdad a sus átomos que torne verdadera a la proposición. De esta manera Cook nos brinda un modo para demostrar si un problema dado es $\mathcal{NP}$-Completo. Fue esta herramienta la utilizada por Karp para demostrar que otros 20 problemas combinatorios pertenecen a la clase de problemas $\mathcal{NP}$-Completos [**?**].

Todo hace pensar que los problemas $\mathcal{NP}$-Completos son intratables, aunque actualmente no se ha hecho ningún avance en la demostración o refutación de este enunciado. Sí se ha incrementado la lista de los problemas que pertenecen a dicha clase, ya que cada vez más problemas independientes son demostrados pertenecer a ella [**?**].

1.3. Sistemas Binarios Estocásticos

Definición 1.3.1 (Sistema Binario Estocástico) *Un Sistema Binario Estocástico (SBE) se define a partir de una terna (T, ϕ, P), utilizando la terminología de Ball [**?**]:*

1. $T = (t_1...t_n)$ *conjunto ordenado de n componentes del sistema*
2. $P = (p_1...p_n)$ *las probabilidades de operación de cada elemento del sistema modelados con variables aleatorias de Bernoulli independientes*
3. $\phi : \{0,1\}^n \longrightarrow \{0,1\}$ *la función estructura del sistema que toma como valores 0 y 1, donde dada una configuración $x = (x_1...x_n)$, $\phi(x) = 1$ si el sistema se encuentra funcional dado el estado x o $\phi(x) = 0$ en caso contrario.*

Un sistema binario es monótono si ϕ es monótona. Por monotonía nos referimos a que, dado un orden relativo entre dos configuraciones $x = (x_1...x_n)$ e $y = (y_1...y_n)$, como $x \leq y$ si $\forall i$ $x_i \leq y_i$, entonces $\phi(x) \leq \phi(y)$.
En un SBE monótono, un conjunto de corte es un subconjunto de componentes de T tales que cuando fallan aseguran que el sistema esté en estado de falla, sin importar el estado del resto de sus componentes. Por otro lado, una configuración operativa x es minimal cuando $\phi(x) = 1$ y $\phi(x') = 0$ para cada estado x' tal que $x'_i \leq x_i$. Estos estados minimales son los que de alguna forma determinan la estructura del sistema.

Definición 1.3.2 (Confiabilidad de un SBE) *La confiabilidad de un SBE $(S) = (T, \phi, P)$ es la probabilidad de correcta operación:*

$$r = E(\phi(X)) = P(\phi(X) = 1), \tag{1.1}$$

siendo $X = (X_1, \ldots, X_n)$ un vector aleatorio con coordenadas independientes, tales que $P(X_i) = p_i$.

Diremos que un sistema binario es coherente si ϕ es monótona y además se cumple que $\phi(\vec{0}) = 0$ y $\phi(\vec{1}) = 1$, donde $\vec{0}$ es el vector binario que contiene todos sus elementos en 0 y

$\vec{1}$ el que contiene todos en 1. En algunos textos, dentro de la condición de coherencia se pide además que el sistema no posea elementos irrelevantes, es decir, que no exista x_i tal que $\phi(x)$ se mantiene constante para toda configuración x posible indistintamente de si $x_i = 0$ o $x_i = 1$.

A continuación se brinda una lista de ejemplos de Sistemas Binarios Estocásticos considerados en la literatura especializada, junto con sus citas correspondientes:

- Confiabilidad en todos los terminales: dado un grafo aleatorio con fallas en sus elementos, definimos la función estructura del sistema que toma valor 1 si todos los nodos del grafo permanecen conectados, es decir existe algún camino entre todo terminal, y 0 en caso contrario. Este modelo es monótono en el caso donde solo caen aristas y no lo es en el caso de caída de nodos [**?**].

- Dado un grafo 2-nodo conexo G, donde la función estructura determina si un grafo resultante definido por un estado contiene o no dos caminos disjuntos entre todo par de nodos. Un SBE que puede ser de utilidad para el diseño topológico de redes, donde la red asegura la comunicación incluso luego de la eliminación de cualquier elemento. Este modelo es monótono.

- Consideremos un sistema cuya operación requiere k componentes idénticos en funcionamiento. Un modelo de redundancia n posee $n \geq k$ componentes idénticos con probabilidades de operación p. La función estructura vale 1 si y solo si al menos k componentes se mantienen operativos. Este modelo se conoce en la literatura como "k-out-of-n". La confiabilidad del sistema se mide con la probabilidad de que al menos k elementos se mantengan operativos. Dado que la probabilidad de que k elementos fijos se mantengan operativos es p^k, entonces la confiabilidad del sistema será la suma de las combinaciónes de todos los posibles k, es decir $R(k,n) = \sum_{i=k}^{n} \binom{n}{i} p^i (1-p)^{n-i}$ y es un modelo monótono [**?**].

- El mismo sistema anterior pero la función estructura vale 1 si y solo si al menos k de los m componentes del sistema fallan. La anticonfiabilidad del sistema será entonces $R(k,n) = \sum_{i=k}^{n} \binom{n}{i} p^{n-i} (1-p)^i$ y es también un modelo monótono.

- Confiabilidad diámetro acotada [**?**]: dado un grafo aleatorio y un set K de nodos distinguidos el sistema está operativos si todo par de nodos objetivos del conjunto K se encuentran comunicados entre sí por al menos un camino de largo menor o igual a D luego de removidas las aristas que fallaron. Este modelo es monótono en el caso donde solo caen aristas y no lo es en el caso de caída de nodos.

- Dado un grafo aleatorio donde las fallas se producen en las aristas y una función estructura que vale 1 si dado un estado la cantidad de aristas incidentes en todos los nodos del grafo inducido es impar. Este SBE no cumple la condición de monotonía.

Parte II

Confiabilidad en redes

2

Modelos de Confiabilidad

2.1. Introducción

El cálculo de la anticonfiabilidad de una red tiene múltiples aplicaciones de uso, para el funcionamiento del tendido de una red eléctrica, de un sistema de transporte urbano o para el de una red tradicional de servidores y terminales [**?**]. Para representar la red se modela con un grafo donde se distinguen los puntos (representados como nodos) relevantes, los cuales determinan en base a su conectividad o no, el funcionamiento de la red. El estado de la misma se describe mediante un modelo probabilístico que asigna una probabilidad de falla a cada uno de sus componentes. En el caso de una red de comunicación, los nodos representan los terminales de los usuarios, servidores, routers, etc. y los enlaces representan las líneas de comunicación entre ellos. El problema combinatorio del cálculo de la anticonfiabilidad de una red es catalogado como $\mathcal{NP}$-difícil [**?**].

Una red de comunicación puede ser modelada mediante un grafo no dirigido probabilístico sin lazos $G = (V, E)$, siendo V y E el conjunto de nodos y enlaces respectivamente. La medida de confiabilidad asociada depende del conjunto de nodos $K \subseteq V$ que se desean comunicar, del modelo probabilístico que describe su funcionamiento y de la probabilidad de falla de cada componente.

Se plantean algunos modelos posibles:

1. Modelo Clásico: sea $G = (V, E)$ un grafo simple, $K \subseteq V$ el conjunto de terminales y $p : E \to [0, 1]$ la probabilidad de operación de las aristas. Se considera el grafo aleatorio $\mathcal{G} = (V, \mathcal{E})$, donde el conjunto aleatorio de aristas $\mathcal{E}$ responde a la ley de probabilidad p. La confiabilidad clásica $R(K, G, p)$ es la probabilidad que todos los terminales permanezcan comunicados en el grafo $\mathcal{G}$.

2. Modelo de Aristas y Nodos: al modelo anterior se agregan fallas en todos los nodos, por lo que $p : E \cup V \to [0, 1]$, y los nodos también pueden fallar en el grafo aleatorio $\mathcal{G} = (\mathcal{V}, \mathcal{E})$. Cuando un nodo cae también lo hacen todos sus enlaces incidentes.

3. Diámetro Confiabilidad de Redes: al modelo clásico se le considera además un entero positivo d, denominado diámetro. La diámetro confiabilidad de redes es la probabilidad de que todo par de terminales permanezcan comunicados en el grafo aleatorio por caminos de largo d o menores.

4. Modelo Hostil: es un caso especial del modelo de aristas y nodos donde se asume que $p(v) = 1$ para todo nodo terminal $v \in K$.

Este trabajo se centra en el estudio del modelo Hostil. Una discusión a fondo de modelos de confiabilidad de redes se puede encontrar en el libro [**?**]. La confiabilidad de la red se define como la probabilidad de que dado un estado del sistema definido por el vector $x = (x_1...x_n)$ el sistema se mantenga operativo, sendo n la cantidad de componentes del sistema. Para cada elemento factible de falla del sistema, x_i representa la variable aleatoria de Bernoulli que define el estado del elemento, donde $x_i = 1$ si el componente está operativo y $x_i = 0$ si falla. Las aristas y nodos de G fallan como variables aleatorias de modo que:

$$P(x_i = 1) = p_i$$

$$P(x_i = 0) = 1 - p_i = q_i$$

$$P(X = x) = \prod_{i/x_i=1} p_i \prod_{i/x_i=0} q_i$$

Dado el espacio de vectores de $\Omega = \{0, 1\}^n$, sabemos que $|\Omega| = 2^n$ ya que cada componente del sistema tiene dos posibles estados. Luego, utilizando la función estructura $\Phi(X)$ que aplica sobre la variable aleatoria X, definimos la confiabilidad de este modelo como:

$$R_K(G) = P(\Phi(X) = 1)$$

Definimos además el complemento de la medida de confiabilidad, la probabilidad de falla de la red, denominada medida de anticonfiabilidad de G como:

$$U_K(G) = 1 - R_K(G)$$

A lo largo de este documento asumiremos que los nodos terminales son perfectos, por lo que $n = |V| + |E| - |K|$, ya que a pesar de estar trabajando con el modelo hostil, no consideraremos el total de los nodos como factibles a fallas. Los motivos los expondremos en secciones posteriores.

2.2. Métodos de cálculo exacto

2.2.1. Método de Enumeración Exhaustiva

El método de Enumeración Exhaustiva es el método mas básico del cálculo de confiabilidad. Se trata de enumerar todas las posibles combinaciones de estados de la red, calcular su probabilidad de ocurrencia y sumarlas. La formulación es aplicable tanto para el modelo tradicional como al hostil:

$$R_K(G) = \sum_{x:\Phi(x)=1} P(X = x) = \sum_{x:\Phi(x)=1} p^{|\{i:x_i=1\}|}(1-p)^{|\{i:x_i=0\}|}$$

La cantidad de sumandos es exponencial en función del tamaño de la entrada, en este caso elementos factibles de falla, lo que lo hace computacionalmente prohibitivo para grafos de gran tamaño.

2.2.2. Método de Inclusión-Exclusión

El método de inclusión exclusión consiste en identificar todos los cortes minimales del grafo y calcular la probabilidad de que alguno de ellos permanezca activo. Supongamos que tenemos todos los cortes minimales posibles, $\{C_1...C_h\}$, sea A_i el evento donde todos los enlaces del corte C_i operan, entonces tenemos que la probabilidad de que alguno de estos eventos ocurra es:

$$U_K(G) = \sum_{i=1}^{r} (-1)^{(i-1)} \sum_{B\subseteq\{1,...,r\},|B|=i} P(\cap_{j\in B} A_i)$$

la cantidad de cortes minimales puede ser exponencial, por lo que la solución, aunque puede mejorar en cómputo frente a la enumeración completa, sigue manteniendo en el peor caso, el mismo orden.

2.2.3. Método de factorización

Este método consiste en reducir recursivamente el tamaño de los grafos de manera de minimizar la cantidad de sumandos respecto al método de enumeración completa:

$$R_K(G) = p_e R_K(G_e) + (1-p_e) R_K(G-e)$$

Donde G_e es el grafo resultante luego de contraer la arista e (marcarla como operativa) en G y $G-e$ el grafo resultante de eliminar la arista e del grafo G. La principal mejora de este método respecto a la enumeración completa, es la capacidad de detectar previamente si G_e se encuentra K-conectado (los nodos terminales se encuentran conectados con probabilidad 1) luego de fijar la arista e, o si $G-e$ está K-desconectado (los nodos terminales se encuentran desconectados con probabilidad 1) luego de eliminar la misma arista. Esto generalmente aporta una poda al recorrido binario que se realiza sobre todos los elementos de G y que permite un ahorro imporante de cálculo. Se deduce de esto que una adecuada elección de la arista/nodo pivot acelera el tiempo de cómputo del método. Satyanarayana y Chang en su artículo [**?**] demuestran la importancia de seleccionar esta arista en base a propiedades de dominancia de grafos. A pesar de este ahorro de cálculo, es fácil notar que el orden del algoritmo es también exponencial, ya que en el peor de los casos, se enumeran todos los estados posibles del vector de enlaces-nodos.

2.3. Métodos aproximados

La complejidad computacional intrínseca al cálculo de confiabilidad del modelo hostil promueve el desarrollo de métodos de aproximación. Las siguientes definiciones son de utilidad a la hora de comparar distintos métodos estadísticos de estimación puntual de la confiabilidad. Denotaremos mediante γ a la anticonfiabilidad, o parámetro que se desea estimar.

Definición 2.3.1 (Error Relativo) *Dado un nivel de confianza α, el error relativo del estimador (RE por sus siglas en inglés) es el radio del intervalo de confianza para γ, dividido entre el valor real γ.*

Definición 2.3.2 (Error Relativo Acotado) *Decimos que un estimador de la anticonfiabilidad verifica la propiedad de error relativo acotado (BRE por sus siglas en inglés) si su error relativo permanece acotado cuando γ tiende a 0.*

Definición 2.3.3 (Error Relativo Desvaneciente) *Decimos que un estimador de la anticonfiabilidad verifica la propiedad de error relativo desvaneciente (VRE por sus siglas en inglés) si su error relativo tiende a cero cuando γ tiende a 0.*

2.3.1. Método de Monte Carlo Crudo

El método de Monte Carlo Crudo es uno de los más conocidos en la estimación de parámetros y es la base de muchos otros métodos [**?**]. En CMC (por su abreviatura en inglés) en cada paso se genera una muestra independiente e idénticamente distribuida del parámetro a estimar, como por ejemplo la probabilidad de ocurrencia de un evento. Luego, como estimador del parámetro se utiliza el promedio de ocurrencias del evento considerando una muestra iid. Para el caso de la estimación de la anticonfiabilidad de un red se toma una muestra de tamaño N de estado de los enlaces y nodos del grafo representativo de la red. Para obtener cada muestra se ejecutan M pruebas de Bernoulli, donde M representa la cantidad de elementos sorteables de la red. Asumiendo probabilidad de operación uniforme, se realizan M pruebas de Bernoulli. Se dispone luego de una muestra independiente $X_1, \ldots, X_N$, donde cada $X_j = (X_j^1, \ldots, X_j^M)$ es un vector aleatorio que describe los componentes en operación y respeta la ley del vector p. La estimación de confiabilidad mediante CMC es la siguiente:

$$R_{CMC} = \frac{1}{N} \sum_{j=1}^{N} \phi(X_j)$$

Por la ley fuerte de los grandes numeros el promedio converge casi seguramente a R_{CMC} converge casi seguramente a $E(\phi(X))$, es decir, a la confiabilidad del SBE. El estimador representa la proporción de estados de falla de la red sorteados en las N muestras, y al ser un promedio muestral es insesgado y su error cuadrático medio coincide con su varianza.
Por lo tanto la varianza de nuestro estimador será:

$$Var(\overline{Y_N}) = \frac{R_K(G)(1 - R_K(G))}{N}$$

Dado que nuestro sistema es monótono, la anticonfiabilidad de la red tiende a cero a medida que las probabilidades de operación de los elementos se acercan a uno. Hay cierta relación entre la cantidad de muestreos necesarios para asegurar un error relativo debajo de cierta cota dado un nivel de confianza α. Si llamamos γ a la anticonfiabilidad, utilizando el Teorema Central del Límite tenemos que el radio ϵ centrado en el promedio muestral $\overline{Y_N}$ vale:

$$\epsilon = \frac{z_{\alpha/2}\sqrt{\gamma(1-\gamma)}}{\sqrt{N}\sqrt{\gamma}}$$

Y el error relativo definido como el cociente entre el radio de confianza y el valor del estimador, cuando la anticonfiabilidad se torna un evento raro, es decir $\gamma \to 0$:

$$RE(N) = \frac{z_{\alpha/2}\sqrt{(1-\gamma)}}{\sqrt{N}\sqrt{\gamma}} \approx \frac{z_{\alpha/2}}{\sqrt{N}\sqrt{\gamma}} \to +\infty$$

Es importante notar que CMC no cumple la propiedad de BRE, es decir, mantener el error relativo acotado, ni mucho menos con la propiedad del error relativo desvaneciente. A este problema se le conoce como el **problema central de eventos raros**, y es la causa del pobre desempeño de CMC bajo estos contextos.

CMC en el Modelo Hostil

No es necesaria una adaptación específica para el modelo hostil más que la consideración de los nodos como elementos sorteables ya que el método es aplicable tanto en uno como en otro modelo.

CMC Monte Carlo Crudo

Require: $N, G(V,E), K, P = (p_1 ... p_M)$
Ensure: $U_K(G), V_K(G)$
1: $S_1 = 0$
2: **for** $j = 1$ TO N **do**
3: Sorteamos x_j
4: **for** $i = 1$ TO M **do**
5: Sortear x_{ji}.
6: **end for**
7: $S_1 = S_1 + \Phi(x_j)$
8: **end for**
9: $U_K(G) = \frac{S_1}{N}$
10: $V_K(G) = U_K(G)\frac{1-U_K(G)}{N-1}$
11: **return** $U_K(G), V_K(G)$

El problema de Monte Carlo Crudo reside en los escenarios donde las redes son altamente confiables, y en donde su desempeño decae conforme la anticonfiabilidad de la red tiende a cero. Un buen enfoque para la estimación de la anticonfiabilidad cuando la falla de la red es un evento

raro, es a través de los métodos que ponen foco en la reducción de la varianza. Mediante ellos se logra reducir la varianza en tiempos de cálculo similares respecto a CMC al emplear técnicas de muestreo más sofisticadas. Algunas son generalizables a cualquier contexto de estimación de probabilidades en eventos raros, como el Muestreo por Importancia, y otras son más específicas al problema de la confiabilidad de redes como el método Recursivo de Reducción de la Varianza. A continuación describiremos ambos métodos desarrollados para el modelo tradicional, junto con las adaptaciones necesarias para su aplicación al modelo hostil.

2.3.2. Método Recursivo de Reducción de la Varianza

El método recursivo de reducción de la varianza, RVR por sus siglas en inglés fue propuesto originalmente por Mohamed El Khadiri y Héctor Cancela para el modelo de confiabilidad clásica [**?**]. Allí sus autores demuestran que el nuevo estimador propuesto es insesgado y presenta error cuadrático medio siempre inferior que en CMC. Mostraremos luego que el método RVR es insesgado. Detalles sobre el cálculo de varianza y esfuerzo computacional de RVR se pueden encontrar en [**?**] [**?**].
El método fue propuesto inicialmente para probabilidades de operación posiblemente heterogéneas p_i para los enlaces de un grafo simple $G = (V, E)$, donde la confiabilidad se define como la probabilidad de que un conjunto de nodos distinguidos $K \subseteq V$, denominados terminales, se mantengan comunicados. Nuevamente, llamaremos $R_K(G)$ a la probabilidad de comunicación de estos nodos.
Bajo la hipótesis del modelo tradicional, donde sólo fallan aristas y no los nodos, la idea general del método consiste en separar el universo de posiblidades en eventos mutuamente excluyentes y exhaustivos.
Dado un corte C de la red, se define un orden relativo entre las aristas $e_1...e_{|C|}$ del corte. El método consiste en dividir el espacio Ω, en los eventos $\{A_C, B_1...B_m\}$, donde A_C representa el evento donde ocurre el corte C y B_i es el evento donde la arista e_i opera y las aristas $\{1...e_{i-1}\}$ no, para luego condicionar sobre estos eventos e iterar recursivamente sobre los grafos inducidos: $G_i = G - e_1 - .... - e_{i-1} * e_i$.

Definimos $Y = 1-\Phi(X)$ como la anticonfiabilidad del grafo inicial e $Y_i = 1-\Phi(X_i)$ como la anticonfiabilidad de los grafos inducidos por B_i. Dado que los B_i son eventos exhaustivos, podemos reformular la anticonfiabilidad como:

$$Y = A_C \cup \cup_{i=1}^{l} A_C^C \cap B_i \cap \{Y_i\}$$

Es decir, definimos la anticonfiabilidad de la red inicial, como la suma de las descomposiciones condicionadas a los eventos A_C y B_i, y los grafos inducidos por ellos. Inicialmente, el método diferencia dos eventos: cuando ocurre A_C y cuando no. En función de esto puede definir la anticonfiabilidad del grafo como:

$$U_K(G) = P(A_C) + (1 - P(A_C))(P(\Phi(X) = 1/E_{A_C}^C))$$

El cálculo de $P(A_C)$ es trivial, pero no lo es así el cálculo de $P(\Phi(X) = 1)$ sabiendo que no ocure A_C, de aquí que RVR busca estimarlo.

El método consiste en partir el espacio en intervalos que representan la ocurrencia de cada B_i. Para esto, dividimos el intervalo $[0, 1]$ como $P(B_i)/(1 - P(A_C))$, cubriendo así todo el espacio de posibilidades cuando asumimos que no ocurre A_C. Estos intervalos ordenados los denominaremos J_i, donde cada uno se corresponde con cada B_i. Luego, nos valemos de una variable aleatoria U uniforme en $[0, 1]$ y definiremos una nueva variable aleatoria Z como combinación de estos elementos que luego probaremos tiene el mismo valor esperado que la variable Y.

Tenemos entonces que Y_i es la anticonfiabilidad del grafo inducido por el evento B_i, es decir $\Phi_i(X_i)$. Luego el método se define recursivo sobre Y_i, ya que para estimar esta nueva confiabilidad sobre el grafo inducido B_i de tamaño menor que el grafo G inicial, utilizaremos la siguiente formulación recursiva de la variable alealtoria Z definida como:

$$Z = F(G, K) = P(A_C) + (1 - P(A_C)) \sum_{1}^{|A_C|} 1_{(U \in J_i)} F(G_i, K_i)$$

donde:

1. U es una variable aleatoria con distribución uniforme en $[0, 1]$.
2. J_i con $1 \leq i \leq |A_C|$ una secuencia de intervalos disjuntos de amplitud $\frac{P(A_i)}{1-P(A_C)}$
3. $1_{(U \in J_i)}$ la indicatriz que determina el intervalo J_i y el corte B_i bajo el cual se continuará la recursión.

Probaremos que Z así definida tiene el mismo valor esperado que Y. Dado que $P(Y = 0|A_C) = 0$ y que además Y es binaria y $E(Y|A_C) = 1$ tenemos que:

$$U_K(G) = E(Y) = P(A_C) + (1 - P(A_C)) \sum_{i=1}^{l} P(B_i)/(1 - P(A_C))E(Y|B_i)$$

$$= P(A_C) + (1 - P(A_C)) \sum_{i=1}^{l} P(U \in J_i)E(Y|B_i)$$

$$= P(A_C) + (1 - P(A_C)) \sum_{i=1}^{l} E(1_{(U \in J_i)})E(Y|B_i)$$

También tenemos que $E(Y|B_i) = E(1 - \Phi(X)|B_i) = E(1 - \Phi(X)) = E(Y_i)$.
Sustituyendo:

$$U_K(G) = P(A_C) + (1 - P(A_C)) \sum_{i=1}^{l} E(1_{(U \in J_i)})E(Y_i)$$

$$= P(A_C) + (1 - P(A_C)) \sum_{i=1}^{l} E(1_{(U \in J_i)} Y_i)$$

$$= E(P(A_C) + (1 - P(A_C)) \sum_{i=1}^{l} 1_{(U \in J_i)} Y_i)$$

$$= E(Z)$$

Repitiendo el proceso anterior N veces se muestrea la nueva variable aleatoria que al ser insesgada respecto al valor de la anticonfiabilidad de la red nos permite lograr un estimador de la misma a través del promedio. A su vez El Khadiri y Cancela [**?**] prueban que el método mejora su varianza con respecto a CMC.

RVR en el Modelo Hostil

La adaptación realizada al algoritmo para el modelo hostil consiste en considerar tanto en los cortes como en la posterior división del espacio del evento donde no ocurre A_C, los nodos no terminales factibles de falla.

Dado un corte C, el cual incluye nodos y aristas, definimos nuevamente un orden relativo entre los elementos $e_1 ... e_{|C|}$ del corte. Los eventos B_i definidos por este nuevo corte cumplen con la propiedad de ser mutuamente excluyentes y exhaustivos. Definimos la variable aleatoria Z y la función $F(G, K)$ recursiva que la muestrea de manera análoga que en el modelo tradicional. La demostración de que $F(G, K)$ es un estimador insesgado para $U(G, K)$ es análoga al modelo anterior ya que se cumplen las mismas hipótesis.

RVR Reducción Recursiva de la Varianza

Require: $N, G(V, E), K, P = (p_1 ... p_M)$
Ensure: $U_K(G), V_K(G)$
1: $S_1 = 0$
2: $S_2 = 0$
3: **for** $j = 1$ TO N **do**
4: $\quad \tilde{R_K}(G) =$ RecursiveRVR(G, K, P)
5: $\quad S_1 = S_1 + \tilde{R_K}(G)$
6: $\quad S_2 = S_2 + \tilde{R_K}(G)^2$
7: **end for**
8: $U_K(G) = \frac{S_1}{N}$
9: $V_K(G) = \frac{S_2 - \frac{S_1^2}{N}}{N(N-1)}$
10: **return** $U_K(G), V_K(G)$

Recursive RVR Procedimiento Recursivo
Require: $G(V, E), K, P = (p_1...p_M)$
Ensure: $U_K(G)$
if G es K-conexo **then**
  return 0
else
  if G es K-disconexo **then**
    return 1
  else
    C = HallarCorteDeMaxProbabilidad(G)
    Calcular $P(C)$
    Sortear U Uniforme$[0, 1]$
    Tomar B_i con $U \in J_i$
    Calcular B_i
    $G_i =$ ContraerGrafo(G, B_i)
    $U_K(G) = P(C) + P(B_i)$RecursiveRVR(G_i, K, P)
    return $U_K(G)$
  end if
end if

Nota: en la siguiente sección presentaremos junto con AZVIS el algoritmo de Ford Fulkerson modificado para caída de nodos (HallarCorteDeMaxProbabilidad) que utilizamos para encontrar los cortes tanto para RVR como para AZVIS.

2.3.3. Método de Muestreo por Importancia

Un escenario muy común en el contexto de las redes es el de las redes altamente confiables donde las probabilidades de falla de cada componente son extremadamente bajas y/o existe alta conectividad entre los nodos terminales. Cuando la falla de la red es un evento raro el método de Monte Carlo en su formulación estándar y otras tantas variaciones se vuelven poco apropiadas para la estimación de la confiabilidad, ya que para obtener una precisión aceptable se requiere un número elevado de replicaciones, lo que los vuelve poco competitivos a nivel de esfuerzo computacional [**?**]. Aquí profundizaremos sobre el método de Muestreo por Importancia, técnica de uso general aplicable a la simulación para la estimación de parámetros que tienden a cero [**?**].

IS, según su sigla en inglés (Importance Sampling), consiste en un cambio en la distribución de probabilidades de falla de los elementos considerados en el muestreo, con el objetivo de incrementar la probabilidad del evento a estimar y así lograr disminuir la varianza.

Denotaremos el nuevo orden de probabilidades como $\tilde{P}$ y P a las distribuciones originales. Definiendo el factor:

$$L(x) = P[X = x]/\tilde{P}[X = x]$$

tendremos entonces que,

$$u = E[\Phi(X)] = \sum_{x \in \{0,1\}^m} \Phi(x) P[X = x] = \sum_{x \in \{0,1\}^m} \Phi(x) \frac{P[X = x]}{\tilde{P}[X = x]} \tilde{P}[X = x]$$

$$= \sum_{x \in \{0,1\}^m} \Phi(x) L(x) \tilde{P}[X = x]$$

donde $L(X)$ es el cociente de verosimilitud entre ambas probabilidades $\tilde{P}$ y P.
Podemos definir el valor esperado de $\Phi(X)$ como la esperanza bajo $\tilde{P}$:

$$u = \tilde{E}[\Phi(X) L(X)]$$

y podremos definir por lo tanto un nuevo estimador del valor esperado:

$$\hat{u} = \hat{E}(\Phi(X) L(X)) = \frac{1}{N} \sum_{j=1}^{N} \Phi(x_j) L(x_j)$$

Donde $\{X_1, \ldots, X_N\}$ es una muestra iid de la variable aleatoria X generadas bajo la nueva distribución $\tilde{P}$. El sesgo introducido por el cambio de probabilidades es corregido por el factor de verosimilitud. La varianza del nuevo estimador será entonces:

$$\tilde{\sigma^2}(\Phi(X) L(X)) = \frac{\tilde{E}[\Phi(X) L(X)^2] - (E[\Phi(X)])^2}{N}$$

esto sugiere que el cambio de probabilidades óptimo para minimizar dicha varianza es:

$$\tilde{P} = \frac{P(X)\Phi(X)}{E[\Phi(X)]}$$

$$\tilde{E}[\Phi(X) L(X)^2] = \tilde{E}[(\frac{\Phi(X) P(X) E(\Phi(X))}{\Phi(X) P(X)})^2] = E^2(\Phi(X))$$

lo que nos daría un estimador con varianza cero. Es decir, que una sola muestra de la nueva distribución nos daría la anticonfiabilidad de la red. El principal problema de esto (y del método en general) es que necesitamos conocer $E[\Phi(X)]$ que es justamente el parámetro que intentamos estimar.

Versión secuencial de IS con varianza cero

L'Ecuyer formula una nueva versión secuencial de IS [**?**], donde el proceso de muestreo del vector X se modela como una cadena de Markov. Los estados de los enlaces $x_1 ... x_m$ son generados secuencialmente en ese orden. En el i-ésimo paso se determina el valor de x_i sobre $\{0, 1\}$ bajo la nueva distribución de probabilidades, dependientes de los valores previos sorteados $x_1 ... x_{i-1}$ con el objetivo de construir el estimador de varianza cero.

Dado un grafo intermedio G', definido por el estado de las variables $x_1...x_{i-1}$, se define la anticonfiabilidad intermedia del mismo como:

$$u_i(x_1...x_{i-1}) = E[\Phi(X)|X_1 = x_1, ..., X_{i-1} = x_{i-1}]$$

Luego se define la nueva probabilidad de distribución del elemento x_i como:

$$\tilde{q_i} = \tilde{P}[\Phi(X)|X_1 = x_1, ..., X_{i-1} = x_{i-1}] = \frac{q_i u_{i+1}(x_1, ..., x_{i-1}, 0)}{u_i(x_1, ..., x_{i-1})}.$$

$$= \frac{q_i u_{i+1}(x_1, ..., x_{i-1}, 0)}{q_i u_{i+1}(x_1, ..., x_{i-1}, 0) + (1 - q_i)u_{i+1}(x_1, ..., x_{i-1}, 1)}$$

Y con esto el cociente de verosimilitud intermedio $L_i(x_i)$ queda definido como:

$$L_i(x_i) = x_i \frac{1 - q_i}{1 - \tilde{q_i}} + (1 - x_i)\frac{q_i}{\tilde{q_i}} = \frac{u_i(x_1, ..., x_{i-1})}{u_{i+1}(x_1, ..., x_{i-1}, x_i)}$$

Y el cociente de verosimilitud genérico como:

$$L(X) = \prod_{i=1}^{m} L_i(x_i)$$

En [**?**] L'Ecuyer demuestra que el estimador construido de esta forma tiene varianza cero. Pero para su implementación nos enfrentamos a un problema similar: necesitamos conocer cada u_i que repesenta la anticonfiabilidad de cada grafo intermedio. En particular $u_0 = U_K(G)$ que es la anticonfiabilidad del grafo G inicial, parámetro el cual intentamos estimar.

Estimadores de u(.) y sus propiedades

Dado que desconocemos las anticonfiabilidades de los grafos intermedios $u_i(.)$, surge la necesidad de hallar una forma eficiente de estimarlos. El objetivo de esto es construir algún estimador $\hat{u}_i(.)$ no muy alejado de los óptimos $u_i(.)$ de forma que, sin lograr el perfecto estimador de varianza cero, poder reducir la varianza de forma significativa.
Plantearemos aquí ciertas hipótesis sobre el estimador concreto de $\hat{u}_i(.)$, que de cumplirse se demuestra en [**?**] que el estimador de la anticonfiabilidad cumplirá con la condición del error relativo acotado e incluso del error relativo desvaneciente. A continuación detallamos tales hipótesis.

1. Para cada $x = (x_1, ..., x_i) \in \{0, 1\}^i, 1 \leq i \leq m$ existe una constante $a_{i+1}(x_1, ..., x_i)$ independiente de la anticonfiabilidad de la red $R_K(G)$ tal que:

$$\hat{u}_{i+1} = a_{i+1}(x_1, ..., x_i)u_{i+1}(x_1, ..., x_i) + o(u_{i+1}(x_1, ..., x_i))$$

2. Dado

$$S_1 = \{x \in \{0, 1\}^m : \Phi(x) = 1 \text{ y } \tilde{P}[X = x] = \Theta(1)\}$$

que representa el conjunto de todos los estados donde la red falla, pero que bajo la nueva distribución $\tilde{P}$ dejan de ser eventos raros. Consideremos las siguientes condiciones para todo $x \in S_1$:

a) $\frac{\hat{u}_{i+1}(x_1,...,x_{i-1},1)}{u_{i+1}(x_1,...,x_{i-1},1)} = \frac{\hat{u}_{i+1}(x_1,...,x_{i-1},0)}{u_{i+1}(x_1,...,x_{i-1},0)} + o(1)$

b) $x_i = 0$
$a_{i+1}(x_1, ..., x_i) = 1$
$(1 - q_i)\hat{u}_{i+1}(x_1, ..., x_{i-1}, 1) = o(q_i\hat{u}_{i+1}(x_1, ..., x_{i-1}, 0))$

c) $x_i = 1$
$a_{i+1}(x_1, ..., x_i) = 1$
$q_i\hat{u}_{i+1}(x_1, ..., x_{i-1}, 0) = o((1 - q_i)\hat{u}_{i+1}(x_1, ..., x_{i-1}, 1))$

Asumiendo que el estimador $\hat{u}_i(.)$ cumple con la propiedad del item 1 se puede demostrar que nuestro estimador para la anticonfiabilidad cumplirá con la propiedad del error relativo acotado. Y que si además de cumplir con el item 1 también cumple al menos con una de las tres propiedades establecidas en 2.a, 2.b o 2.c entonces el estimador también cumplirá con la condición que impone el error relativo desvaneciente [**?**].

Aproximación basada en cortes minimales de IS-AZVIS

En esta implementación de AZVIS se propone utilizar los cortes de máxima probabilidad como estimadores de los u_i intermedios. Llamaremos a estos estimadores $\tilde{u_i}(.)$. Como ya vimos en secciones anteriores, un K-corte de un grafo G es un corte que deja sin conexión a al menos algún par de nodos terminales del grafo. Un K-corte es minimal si solo contiene como corte a si mismo y ningúno más, es decir, ningún elemento del corte "sobra". Para todo K-corte γ definimos el evento $E(\gamma)$ como el evento donde todos los componentes del corte γ fallan, es decir: ocurre el corte. Sabemos que para que la red falle algún corte minimal debe ocurrir por lo que podemos formular la anticonfiabilidad en función de los posibles K-cortes γ minimales:

$$U_K(G) = P[\cup E(\gamma)].$$

Definimos también el corte γ de máxima probabilidad entre los cortes minimales como:

$$\gamma = argmax\{P[E(\acute{\gamma})] : \acute{\gamma} \text{ corte minimal de } G\}$$

Como observamos en la sección anterior en IS-AZVIS para construir $\tilde{q_i}$ en el i-ésimo paso iterativo del algoritmo, debemos estimar de alguna forma la anticonfiabilidad de los grafos intermedios G_i. En cada paso nos vemos en la necesidad de estimar $u_{i+1}(x_1, ..., x_{i-1}, 0)$ y $u_{i+1}(x_1, ..., x_{i-1}, 1)$, en otras palabras estimar la anticonfiabilidad de los grafos G^-_{i+1} definido a partir de G por el vector $(x_1....x_{i-1}, 0)$ y G^+_{i+1} definido por $(x_1....x_{i-1}, 1)$. Esta implementación propone estimar dichos parámetros como $P[E(\gamma^-_i)]$ y $P[E(\gamma^+_i)]$, donde γ^-_i es el corte máxima probabilidad para G^-_{i+1} y γ^+_i para G^+_{i+1}. En [**?**] se provee una prueba de que la aproximación basada en cortes minimales cumple con las hipótesis establecidas en la sección anterior, para que el estimador de IS construido de esta forma cumpla con las propiedad de BRE y VRE.

IS-AZVIS bajo el Modelo Hostil

Dado que IS-AZVIS es un método general para la estimación de eventos raros y que en su construcción utiliza fuertes supuestos sobre los estimadores intermedios, su adaptación al modelo hostil nos resultó un poco más costosa que la de RVR. A continuación se establecen algunos puntos considerados para realizar dicha adaptación:

1. Nos vimos en la necesidad de limitar el modelo de estudio de este trabajo a aquel donde solo fallen los nodos no terminales y donde los terminales son considerados perfectos (al que llamamos modelo hostil). El motivo de esta decisión fue que luego de realizar varias pruebas con el fin de evaluar los algoritmos implementados para el modelo de Aristas y Nodos, AZVIS devolviera resultados negativos. Lo volvimos a corroborar mediante ejecuciones con grafos pequeños que sirvieron de modelos para verificar el correcto desempeño de los algoritmos, en donde el estimador obtenido tenía cierto sesgo con respecto al valor exacto de la anticonfiabilidad. En la sección de resultados presentamos uno de estos grafos y los resultados teóricos al aplicarle IS-AZVIS. La principal sospecha del porqué de la falla del método apunta a que el Sistema Binario Estocástico que representa el modelo hostil no es coherente, ya que pierde la propiedad de la monotonía.
   A modo de ejemplo, supongamos que el elemento i de un grafo dado es un nodo terminal. Consideremos un K-corte del grafo: $x = (x_1...x_{i-1}, 1, x_{i+1}...x_m)$, de manera que todo par de nodos terminales distintos de i permanecen conectados y el terminal i es el que se encuentra desconectado del resto de los terminales y por lo tanto define $\Phi(x) = 0$. Consideremos ahora $x' < x$ construido como $x' = (x_1...x_{i-1}, 0, x_{i+1}...x_m)$. El grafo inducido G' dado por G y x', tendrá todo par de nodos terminales conectados por lo que $\Phi(x') = 1$. De esta manera se contradice la propiedad de monotonía del sistema. Como IS-AZVIS aproxima la anticonfiabilidad de los grafos intermedios G_i con cortes mínimos de máxima probabilidad, utiliza el supuesto de que en cualquier otro estado de la red condicionado al evento del corte la red falla. Eso se cumple por la mencionada propiedad de monotonía del sistema tradicional que deja de ser tal en el modelo de Aristas y Nodos donde los terminales distinguidos fallan.

2. Para la implementación del algoritmo que halla el corte de máxima probabilidad fue necesaria una adaptación del algoritmo tradicional de Ford Fulkerson que aplica solo a grafos con flujos en las aristas. Para lograr esto necesitábamos que el algoritmo incluyera capacidades de flujo en los nodos factibles de fallas, de forma que fuesen considerados en el corte. A continuación se presentan el algoritmo de IS-AZVIS adaptado y en una sección posterior, el algoritmo de Ford Fulkerson adaptado a la caída de nodos utilizado por IS-AZVIS. Es importante aclarar que las modificaciones para adaptar Ford Fulkerson a la búsqueda de cortes de máxima probabilidad fueron introducidas en el marco de este proyecto.

IS-AZVIS Aproximación basado en cortes de máxima probabilidad

Require: $G(V,E), K, P = (p_1 ... p_M)$
Ensure: $U_K(G), V_K(G)$
$S_1 = 0$
$S_2 = 0$
for $j = 1$ TO N **do**
  $G_{Iter} = G$
  $L_j(x) = 1$
  for $i = 1$ TO M **do**
    $G_{i-Opera}$ = fijar i operativo en G
    $G_{i-NoOpera}$ = fijar i no operativo en G
    $u_{i-Opera}$ =CalcularCorteDeMaxProbabilidad($G_{i-Opera}$)
    $u_{i-NoOpera}$ =CalcularCorteDeMaxProbabilidad($G_{i-NoOpera}$)
    $q_i = 1 - p_i$
    $\hat{q}_i = (q_i u_{i-noOpera})/(q_i u_{i-noOpera} + (1 - q_i) u_{i-Opera})$
    Sortear x_{ij} bajo $\hat{q}_i$
    if $x_{ij} = 1$ **then**
      $G_{iter} = G_{i-Opera}$
    else
      $G_{iter} = G_{i-noOpera}$
    end if
    $L_j(x_i) = x_{ij} \frac{1-q_i}{1-\hat{q}_i} + (1 - x_{ij}) \frac{q_i}{\hat{q}_i}$
    $L_j(X) = L_j(X) L_j(x_i)$
  end for
  $S_1 = S_1 + \Phi(X_j) L_j(X)$
  $S_2 = S_2 + \Phi(X_j) L_j(X)^2$
end for
$U_K(G) = \frac{S_1}{N}$
$V_K(G) = \frac{S_2 - S_1^2/N}{N(N-1)}$
return $U_K(G), V_K(G)$

2.4. Análisis de falla IS-AZVIS bajo el modelo de Aristas y Nodos

En esta sección analizaremos el comportamiento de IS-AZVIS sobre un grafo simple del modelo de Aristas y Nodos donde fallan tanto nodos como aristas, y donde la falla también puede ocurrir en los nodos distinguidos.
Consideremos el siguiente grafo:

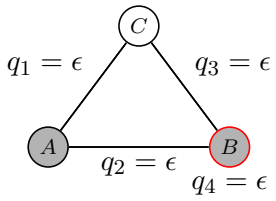


Figura 2.1:
$|E| = 3$ $K = \{A, B\}$

Donde la probabilidad de falla del nodo B es la misma que la de las aristas: $q_i = \epsilon$ para todo i. Para simplificar el ejemplo asumiremos que los nodos A y C son perfectos, es decir, falla solo el nodo B que además pertenece al conjunto K de los nodos terminales. Definimos un orden para los elementos factibles de fallas del sistema:

- x_1: enlace entre nodos A y C
- x_2: enlace entre nodos A y B
- x_3: enlace entre nodos B y C
- x_4: nodo B

Sabemos que por construcción el método AZVIS en cada paso iterativo estima la anticonfiabilidad $u_{i+1}(.)$ de los grafos intermedios dado por el estado de los i elementos previos. El estimador utilizado para esas anticonfiabilidades intermedias es el corte minimal de máxima probabilidad del grafo G inducido por el vector de estados previos. El lector puede consultar los ejemplos provistos en [**?**] en donde se comparan los estimadores $\hat{u}_{i+1}$ de cada grafo intermedio con las anticonfiabilidades reales y en todos los casos coinciden o tienen una diferencia menor a $o(\epsilon)$. La idea de este ejemplo es de forma análoga mostrarle al lector como en el modelo donde fallan los K terminales las aproximaciones obtenidas a través de los cortes difieren de forma significativa de las anticonfiabilidades ideales, lo que produce estimadores finales sesgados respecto de $R_K(G)$.
Analicemos entonces las anticonfiabilidades $u_{i+1}(.)$ intermedias definidas por los vectores previos de estados $(x_1, ..., x_i)$ y sus respectivas aproximaciones $\hat{u}_{i+1}(x_1, ..., x_i)$ a través de los cortes de máxima probabilidad. De esta forma el vector de estados incluye no solo el estado de los enlaces factibles sino que también el estado del nodo B.

Estado $(x_1, ..., x_i)$	$u_{i+1}(x_1, ..., x_i)$	$\hat{u}_{i+1}(x_1, ..., x_i)$
(0)	$\epsilon(1-\epsilon)$	ϵ
(1)	$\epsilon^2(1-\epsilon)$	ϵ^2
(0,0)	$1-\epsilon$	1
(1,0)	$\epsilon(1-\epsilon)$	ϵ
(0,1)	0	0
(1,1)	0	0
(0,0,0)	$1-\epsilon$	1
(0,1,0)	0	0
(0,0,1)	$1-\epsilon$	1
(0,1,1)	0	0
(1,0,0)	$1-\epsilon$	1
(1,1,0)	0	0
(1,0,1)	$1-\epsilon$	1
(1,1,1)	0	0

Para cada estado la aproximación utilizada para la anticonfiabilidad del subgrafo mantiene en todos los casos un sesgo dado por $(1-\epsilon)$, que es la probabilidad de que el nodo B no falle y es un evento necesario para que cualquier K-corte desconecte los terminales. Esto se debe a que en los casos en que el nodo terminal B falla la red vuelve a un estado operativo sin importar el corte que se considere, ya que el único terminal que permanecería activo en el grafo sería el nodo A (y un grafo que contiene un único terminal es K-conexo siempre, es decir $\Phi(x) = 1$ para todo estado x). De esta manera la anticonfiabilidad de la red se vuelve nula en tales casos. Dado que los estimadores de anticonfiabilidad intermedios presentan una desviación de orden mayor que ϵ, es natural que AZVIS construido de esta manera no sea válido como método de aproximación para el modelo de Aristas y Nodos.

Se puede apreciar que una aproximación a la solución de este problema podría desarrollarse si se considerase junto con los cortes el evento donde al menos un par de los K nodos que un corte de máxima probabilidad desconecta se mantengan operativos. De esta forma podríamos asegurarnos que el corte realmente cumpla la función de desconectar algún par de nodos terminales. Esto podría analizarse en trabajos futuros con el objetivo de encontrar una variación de AZVIS aplicable al modelo de Aristas y Nodos.

2.4.1. Algoritmos utilizados

En esta sección enumeramos los algoritmos auxiliares más importantes utilizados por los métodos de aproximación implementados. Entre ellos se incluyen: Ford Fulkerson adaptado para hallar cortes de máxima probabilidad teniendo en cuenta fallas en los nodos, recorridas en anchura para identificar caminos entre dos nodos dados y DFS para conocer si dado un grafo y un estado, el mismo posee los terminales conectados o no.

2.4.1.1. Búsqueda en Anchura, BFS

Algoritmo que recibe como parámetros de entrada: $G = (V, E)$, $v \in V$ y devuelve una lista que indica para cada nodo de V si fue alcanzado desde v o no.

BFS Breadth First Search Hostil

Require: $G(V, E), v \in V$
Ensure: Lista de Padres P
1: Crear lista P vacia
2: Crear lista Q vacia
3: Agregar v a Q
4: **while** queden elementos en Q **do**
5: Quitar elemento u de Q
6: Marcar u como visitado
7: **if** $v = (u, w)$ está activo y nodo w está activo y w no fue visitado **then**
8: Agregar w a Q
9: Guardar $P(w) = u$
10: **end if**
11: **end while**
12: **return** P

2.4.1.2. Ford Fulkerson adaptado

Algoritmo que recibe como parámetros de entrada: $G = (V, E)$, M (matriz de flujo asociada), $v, s \in V$ y retorna el corte de máximo flujo entre los nodos v y s incluyendo tanto nodos como aristas. Para lograrlo fue necesario ampliar el algoritmo tradicional de Ford Fulkerson que trabaja solo con flujos sobre aristas. La idea en términos generales es la de en cada paso iterativo al calcular el camino de flujo máximo entre v y s incluir las capacidades de los nodos intermedios de este camino en el cálculo del flujo. De la misma manera, al modificar las capacidades de las aristas con el valor del flujo máximo hallado, también modificar las capacidades de los nodos intermedios. Así, al calcular el corte en base a los elementos de capacidad residual nula en la matriz residual resultante incluiremos también nodos obteniendo así un corte que incluya tanto aristas como nodos.

Ford Fulkerson Ford Fulkerson Hostil

Require: $G(V, E), M, s, v \in V$
Ensure: Lista C con el corte de máxima probabilidad entre s y v
1: $padres$ = BFSHostil(G, s)
2: **while** exista camino entre s y $t \equiv t \in padres$ **do**
3: F = Calcular el máximo flujo entre s y t segun M
4: $u = t$
5: **for** padre w de u **do**
6: $M(w, u) = M(w, u) - F$
7: $M(u, w) = M(u, w) + F$
8: $M(w, w) = M(w, w) - F$
9: $u = w$
10: **end for**

11: Asociar la nueva matrix M a G $padres$ = BFSHostil(G, s)
12: **end while**
13: Calcular corte C a partir de M
14: **return** C

2.4.1.3. Cálculo del corte de máxima probabilidad adaptado

Este algoritmo es el contenedor de Ford Fulkerson Hostil, que dados el grafo $G(V, E)$ y la lista de terminales K, itera sobre todos los pares $s, v \in K$ y calcula los cortes de máxima probabilidad entre cada par utilizando Ford Fulkerson para retornar el de máxima probabilidad entre todos ellos.

CalcularCorteMaxProbabilidad Algoritmo que itera sobre Ford Fulkerson entre todos los pares K y obtiene el corte de máxima probabilidad

Require: $G(V, E), K, P = (p_1...p_M)$
Ensure: C K-corte de máxima probabilidad
1: C vacio
2: Obtener la matriz M de flujo de G
3: **for** todo par (s, t) de K **do**
4: C_{actual} =FF(G, M, s, t, P)
5: $C =$ máx $\{C, C_{actual}\}$
6: **end for**
7: **return** C

Parte III

Resultados Experimentales

3

Resultados

3.1. Métricas

En esta sección presentaremos los resultados numéricos obtenidos aplicando sobre distintos grafos el método de Muestreo por Importancia instanciado en AZVIS por L'Ecuyer, Rubino, Saggadi y Tuffin y el método Recursivo de Reducción de la Varianza por Héctor Cancela y Mohamed El Khadiri para la estimación de la anticonfiabilidad en redes $R_K(G)$. Ambos métodos modificados en este trabajo para ejecutar sobre el modelo hostil con la hipótesis de que los terminales distinguidos no fallan.

Entre las medidas a considerar se encuentran la precisión y el tiempo de cómputo tomando como referencia las medidas de Monte Carlo Crudo. Es decir, tendremos en consideración luego de ejecutar cada algoritmo sobre cada grafo la varianza obtenida, el estimador puntual del parámetro, el tiempo de ejecución en segundos y el coeficiente de eficiencia relativa W. El coeficiente W es una medida útil para comparar directamente los resultados de cada método con el de CMC, Crude Monte Carlo por sus siglas en inglés. Para ello se utilizan el tiempo de cómputo y la varianza de los métodos y se define como:

$$\hat{W}_{\frac{CMC}{ME}} = \frac{\hat{V}_{CMC}.t_{MCC}}{\hat{V}_{ME}.t_{ME}}$$

Donde *ME* instancia al método que se desea comparar contra CMC. En nuestro caso se instanciará como AZVIS y como RVR. Luego, el mismo factor $\hat{W}$ podrá ser utilizado directamente en la comparación entre ambos métodos.
Las pruebas fueron realizadas en una HP Envy NOTEBOOK con una capacidad de 16.0GB de RAM y un procesador Intel(R) Core(TM) i7-6700HQ trabajando a una frecuencia de 2.60GHz. El software que utilizamos fue MATLAB R2015a sobre una plataforma con Windows 7 de 64 bits.

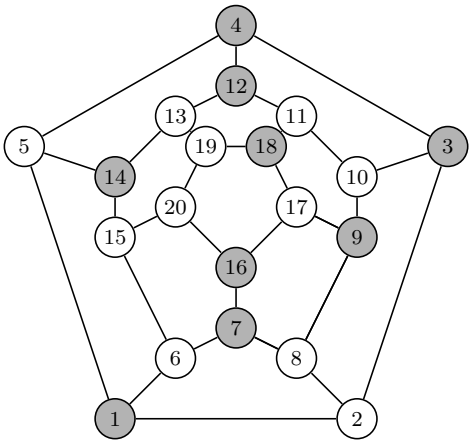
3.2. Grafos utilizados

Para los grafos utilizados se consideran varios de los grafos presentes comúnmente en la literatura sobre el estudio de la confiabilidad en redes, más el agregado de dos casos reales de

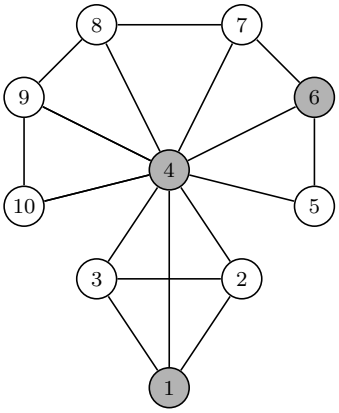
redes como son la Red Oeste y Este de ANTEL. Para todos ellos fueron seleccionados los nodos terminales como los de mayor conectividad (ej, nodos con conectividad mayor o igual que 3), tratando siempre de que la cantidad de nodos terminales no supere el 40 % del total de nodos. Para cada grafo se consideran el conjunto de probabilidades de operaciones tanto de aristas: $p \in \{0{,}95, 0{,}97, 0{,}99\}$ como de nodos no terminales $u \in \{0{,}95, 0{,}97, 0{,}99\}$ siendo estas uniformes para ambos tipos de elementos en cada instancia. Considerando todas las combinaciones posibles posibles tendremos nueve escenarios por grafo. La cantidad de repeticiones N fue tomado como el máximo razonable al que pudieron ser sometidos los grafos seleccionados sin caer en tiempos de ejecuciones prohibitivos para el entorno utilizado: $N = 10^4$.

Características de los grafos:

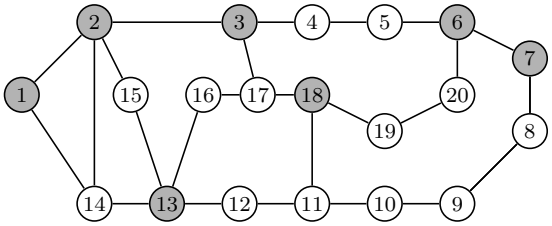
- Grafo RAU $|E| = 10$ $K = \{1, 4, 6\}$
- Grafo Dodecahedro $|E| = 20$ $K = \{1, 3, 4, 7, 9, 12, 14, 16, 18\}$
- Grafo ArpaNet $|E| = 20$ $K = \{1, 2, 3, 6, 7, 13, 18\}$
- Grafo Atlanta $|E| = 15$ $K = \{1, 3, 5, 7, 8, 9, 12\}$
- Grafo Antel Oeste $|E| = 53$ $K = \{5, 6, 13, 19, 33, 34, 36, 52\}$
- Grafo Antel Este $|E| = 59$ $K = \{3, 7, 8, 13, 20, 21, 24, 31, 40, 46, 49, 50, 52, 53, 59\}$



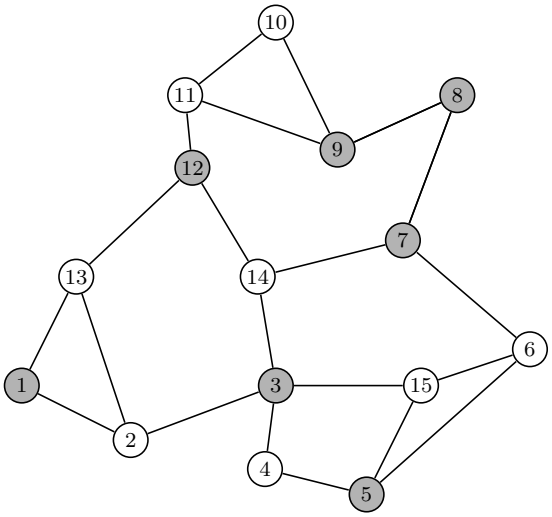
(a) Grafo Dodecahedro



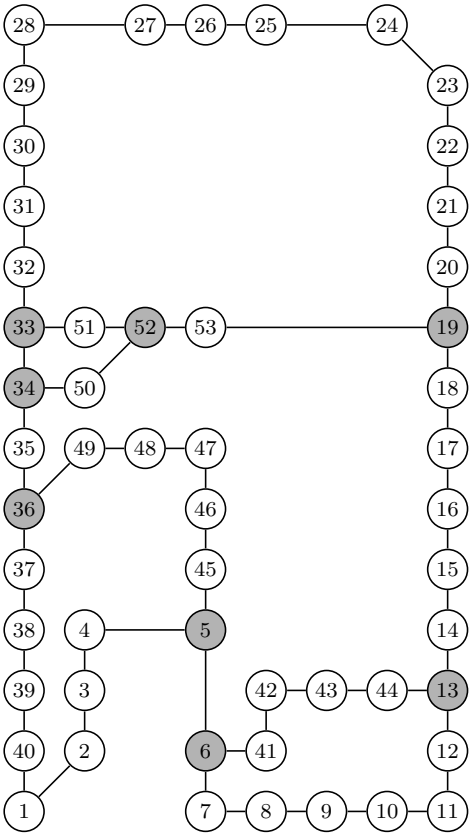
(b) Grafo RAU



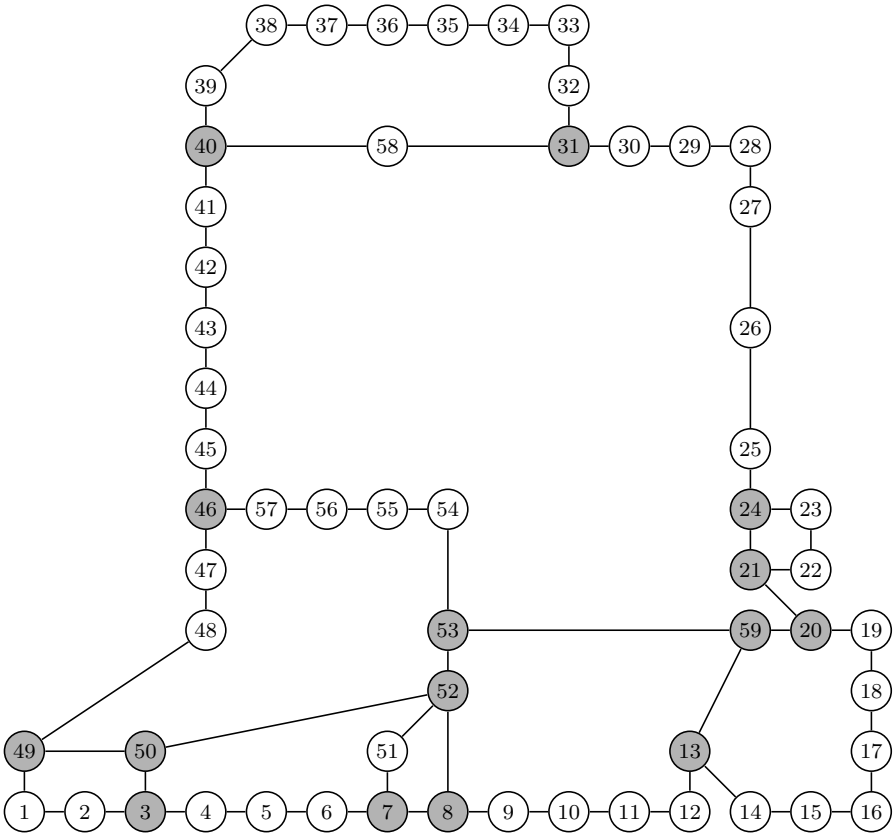
(c) Grafo ArpaNet



(d) Grafo Atlanta



(e) Grafo ANTEL Oeste



(f) Grafo ANTEL Este

3.3. Tablas de resultados

En las tablas de resultados se presenta la siguiente información:

- M: Método a evaluar.
- p: Confiabilidad de las aristas para el caso.
- u: Confiabilidad de los nodos no terminales para el caso.
- N: Tamaño de la muestra para el caso.
- $\hat{U}_K(G)$: estimador de la anticonfiabilidad del grafo.
- $\hat{V}_K(G)$: estimador de la varianza.
- t: tiempo de ejecución del caso.
- $\hat{W}$: coeficiente de performance respecto a CMC.

Grafo RAU							
M	p	u	N	$\hat{U}_K(G)$	$\hat{V}_K(G)$	t	$\hat{W}$
RVR	0.95	0.95	10^4	0.0015939	$6{,}41E-09$	45	21.23
IS	0.95	0.95	10^4	0.0015939	$2{,}02E-09$	539.8	5.62
RVR	0.95	0.97	10^4	0.0010931	$3{,}99E-09$	52.7	1.73
IS	0.95	0.97	10^4	0.00109	$3{,}75E-10$	600	15.98
RVR	0.95	0.99	10^4	0.00078193	$2{,}65E-09$	54	11.53
IS	0.95	0.99	10^4	0.00069164	$4{,}81E-10$	617.7	5.68
RVR	0.97	0.95	10^4	0.00059639	$1{,}23E-09$	53	26.00
IS	0.97	0.95	10^4	0.00054353	$1{,}54E-10$	514.3	21.36
RVR	0.97	0.97	10^4	0.00029026	$4{,}80E-10$	51.2	68.85
IS	0.97	0.97	10^4	0.00034505	$1{,}86E-10$	543.7	16.65
RVR	0.97	0.99	10^4	0.00017382	$2{,}91E-10$	51.8	45.67
IS	0.97	0.99	10^4	0.00017809	$1{,}65E-11$	611.6	66.99
RVR	0.99	0.95	10^4	$8{,}37E{-}5$	$2{,}50E-11$	44.2	333.00
IS	0.99	0.95	10^4	$8{,}49E{-}5$	$1{,}25E-11$	475.2	56.15
RVR	0.99	0.97	10^4	$4{,}15E{-}5$	$1{,}76E-11$	49	395.34
IS	0.99	0.97	10^4	$4{,}33E{-}5$	$3{,}53E-12$	493.3	195.40
RVR	0.99	0.99	10^4	$1{,}19E{-}5$	$8{,}21E-12$	48.5	88.44
IS	0.99	0.99	10^4	$1{,}27E{-}5$	$4{,}45E-12$	547.9	14.48

Grafo Dodecahedro							
M	p	u	N	$\hat{U}_K(G)$	$\hat{V}_K(G)$	t	$\hat{W}$
RVR	0.95	0.95	10^4	0.0090535	$3{,}14E-07$	205.8	1.84
IS	0.95	0.95	10^4	0.0089496	$1{,}22E-07$	2609	37.4
RVR	0.95	0.97	10^4	0.004785	$1{,}07E-07$	306	2.48
IS	0.95	0.97	10^4	0.0047531	$3{,}31E-08$	3550.1	0.69
RVR	0.95	0.99	10^4	0.0019989	$2{,}19E-08$	358	5.41
IS	0.95	0.99	10^4	0.0020218	$1{,}14E-08$	3854.2	0.96
RVR	0.97	0.95	10^4	0.0033151	$1{,}04E-07$	189.5	2.7
IS	0.97	0.95	10^4	0.0032034	$5{,}06E-08$	2201.4	0.48
RVR	0.97	0.97	10^4	0.0012524	$2{,}54E-08$	197.2	5.19
IS	0.97	0.97	10^4	0.00183433	$1{,}72E-08$	2754.9	0.54
RVR	0.97	0.99	10^4	0.00047489	$2{,}30E-10$	321.1	151
IS	0.97	0.99	10^4	0.0006093	$9{,}69E-10$	3965	2.9
RVR	0.99	0.95	10^4	0.00087277	$2{,}95E-10$	137.8	465
IS	0.99	0.95	10^4	0.0009255	$6{,}77E-09$	1556.8	1.78
RVR	0.99	0.97	10^4	0.00025812	$9{,}55E-10$	166.2	71.5
IS	0.99	0.97	10^4	0.00026312	$1{,}61E-10$	1851.9	38
RVR	0.99	0.99	10^4	5.00E-05	$4{,}22E-11$	296.4	147
IS	0.99	0.99	10^4	3.49E-05	$2{,}99E-12$	3049.9	201

Grafo ArpaNet							
M	p	u	N	$\hat{U}_K(G)$	$\hat{V}_K(G)$	t	$\hat{W}$
RVR	0.95	0.95	10^4	0.051351	$1{,}68E-06$	245	2.29
IS	0.95	0.95	10^4	0.036738	$1{,}60E-06$	761.1	0.75
RVR	0.95	0.97	10^4	0.044748	$1{,}17E-06$	214.4	2.78
IS	0.95	0.97	10^4	0.040738	$9{,}32E-07$	865.9	0.86
RVR	0.95	0.99	10^4	0.023175	$3{,}67E-07$	197.1	6.47
IS	0.95	0.99	10^4	0.023244	$5{,}98E-07$	839	0.93
RVR	0.97	0.95	10^4	0.023658	$3{,}13E-07$	196.1	8.37
IS	0.97	0.95	10^4	0.022267	$1{,}07E-06$	806.4	0.59
RVR	0.97	0.97	10^4	0.015214	$4{,}51E-07$	240.3	3.04
IS	0.97	0.97	10^4	0.01694	$3{,}73E-07$	752.8	1.17
RVR	0.97	0.99	10^4	0.0085	$7{,}66E-08$	232.1	9.27
IS	0.97	0.99	10^4	0.0085685	$4{,}28E-08$	865.2	4.45
RVR	0.99	0.95	10^4	0.0078039	$6{,}60E-08$	244	9.55
IS	0.99	0.95	10^4	0.0086097	$7{,}71E-08$	794.9	2.51
RVR	0.99	0.97	10^4	0.00349	$2{,}37E-08$	210.5	16.3
IS	0.99	0.97	10^4	0.0041413	$5{,}82E-08$	811.2	1.73
RVR	0.99	0.99	10^4	0.0011238	$5{,}46E-09$	213.3	20.9
IS	0.99	0.99	10^4	0.0013126	$1{,}06E-09$	813.7	28.2

Grafo Atlanta							
M	p	u	N	$\hat{U}_K(G)$	$\hat{V}_K(G)$	t	$\hat{W}$
RVR	0.95	0.95	10^4	0.11371	$7{,}59E-07$	98.3	1.29
IS	0.95	0.95	10^4	0.092863	$1{,}88E-07$	431.9	1.19
RVR	0.95	0.97	10^4	0.088465	$2{,}68E-07$	116.5	2.63
IS	0.95	0.97	10^4	0.085513	$4{,}91E-07$	520.9	0.32
RVR	0.95	0.99	10^4	0.066285	$1{,}83E-07$	120.6	4.10
IS	0.95	0.99	10^4	0.068603	$8{,}32E-07$	558.9	0.19
RVR	0.97	0.95	10^4	0.084914	$2{,}63E-07$	143.8	2.81
IS	0.97	0.95	10^4	0.09782	$3{,}7E-07$	433.3	0.66
RVR	0.97	0.97	10^4	0.064462	$3{,}56E-07$	130.9	20.9
IS	0.97	0.97	10^4	0.064411	$3{,}20E-06$	445.4	0.68
RVR	0.97	0.99	10^4	0.044238	$2{,}77E-07$	104.1	17.9
IS	0.97	0.99	10^4	0.042384	$2{,}42E-07$	549.3	3.87
RVR	0.99	0.95	10^4	0.061482	$8{,}88E-08$	109.7	57.3
IS	0.99	0.95	10^4	0.066434	$1{,}43E-07$	432.7	9.02
RVR	0.99	0.97	10^4	0.040038	$1{,}36E-8$	111.6	276
IS	0.99	0.97	10^4	0.040906	$1{,}03E-9$	435	966
RVR	0.99	0.99	10^4	0.019947	$2{,}14E-9$	112.4	716
IS	0.99	0.99	10^4	0.023861	$1{,}35E-9$	451.1	283

Grafo Antel Oeste							
M	p	u	N	$\hat{U}_K(G)$	$\hat{V}_K(G)$	t	$\hat{W}$
RVR	0.95	0.95	10^4	0.41953	$1{,}32E-06$	369.8	6.52
IS	0.95	0.95	10^4	0.40769	$1{,}02E-06$	5713.9	0.29
RVR	0.95	0.97	10^4	0.31029	$9{,}05E-05$	472	0.68
IS	0.95	0.97	10^4	0.31433	$2{,}66E-05$	6193.1	0.73
RVR	0.95	0.99	10^4	0.22542	$7{,}50E-05$	441	1.41
IS	0.95	0.99	10^4	0.21542	$8{,}74E-05$	6499.5	0.36
RVR	0.97	0.95	10^4	0.29541	$1{,}26E-05$	384.5	85.2
IS	0.97	0.95	10^4	0.30109	$7{,}48E-05$	5724.3	0.60
RVR	0.97	0.97	10^4	0.19916	$9{,}76E-06$	427.2	10.5
IS	0.97	0.97	10^4	0.22906	$1{,}81E-05$	5245.2	0.20
RVR	0.97	0.99	10^4	0.10498	$3{,}87E-06$	495.1	24.5
IS	0.97	0.99	10^4	0.08054	$2{,}26E-06$	6352.7	0.49
RVR	0.99	0.95	10^4	0.14596	$8{,}11E-06$	369.8	24
IS	0.99	0.95	10^4	0.16962	$1{,}21E-06$	5670	2.85
RVR	0.99	0.97	10^4	0.07284	$1{,}47E-05$	400.2	12.7
IS	0.99	0.97	10^4	0.066295	$5{,}47E-06$	5688.3	1.18
RVR	0.99	0.99	10^4	0.022951	$1{,}70E-05$	598.5	5.69
IS	0.99	0.99	10^4	0.015605	$2{,}75E-06$	6074.5	2.30

Grafo Antel Este							
M	p	u	N	$\hat{U}_K(G)$	$\hat{V}_K(G)$	t	$\hat{W}$
RVR	0.95	0.95	10^4	0.31535	$1{,}51E-04$	4003.1	9.43
IS	0.95	0.95	10^4	0.25630	$1{,}39E-03$	33557.2	0.12
RVR	0.95	0.97	10^4	0.29079	$5{,}96E-05$	5038.4	6.85
IS	0.95	0.97	10^4	0.30184	$9{,}82E-05$	33465.4	0.62
RVR	0.95	0.99	10^4	0.24165	$8{,}70E-05$	4080.1	16.01
IS	0.95	0.99	10^4	0.17547	$9{,}36E-05$	34826.5	1.74
RVR	0.97	0.95	10^4	0.27399	$1{,}21E-04$	3097	8.76
IS	0.97	0.95	10^4	0.19625	$6{,}12E-05$	31574.8	1.69
RVR	0.97	0.97	10^4	0.19527	$1{,}12E-04$	4303	6.75
IS	0.97	0.97	10^4	0.18563	$8{,}43E-05$	30315	2.43
RVR	0.97	0.99	10^4	0.10458	$2{,}26E-05$	5006.1	14.89
IS	0.97	0.99	10^4	0.09526	$2{,}12E-04$	34652.6	0.22
RVR	0.99	0.95	10^4	0.16802	$1{,}01E-04$	4302.8	7.56
IS	0.99	0.95	10^4	0.16962	$1{,}21E-05$	37288	7.26
RVR	0.99	0.97	10^4	0.07284	$1{,}47E-05$	4000.2	5.57
IS	0.99	0.97	10^4	0.069295	$9{,}47E-06$	34874.3	0.99
RVR	0.99	0.99	10^4	0.022951	$1{,}70E-05$	5980.5	3.22
IS	0.99	0.99	10^4	0.021605	$2{,}75E-06$	33699.5	3.53

3.4. Conclusiones

En la mayoría de los resultados obtenidos al correr los algoritmos sobre los seis grafos encontramos una tendencia similar. En primera instancia, es importante notar que los números se diferencian un poco entre los grafos de las redes de Antel (Este y Oeste) y el resto de los grafos (los llamaremos grafos modelos). En casi todos los casos salvo excepciones tanto RVR como AZVIS supera a CMC tomando $\hat{W}$ como comparador. En las redes de Antel CMC supera en varios casos a AZVIS y en alguna excepción a RVR, esto puede tener origen en que dado el tamaño de las topologías en concreto ($|E| > 50$), 10^4 sorteos resultan insuficientes pero dados los tiempos de ejecución fue una limitante real impuesta a este trabajo. También es importante notar que tanto RVR como AZVIS mejoran contra CMC cuando la anticonfiabilidad tiende a cero. Mejoran tanto más que aún en los grafos de Antel para los últimos casos de menor anticonfiabilidad AZVIS logra mejor performance que CMC. En el caso de los grafos modelos esta tendencia es aún más pronunciada, ya que aún en los casos de mayor anticonfiabilidad RVR y AZVIS superan a CMC y esa superioridad se vuelve más notoria a medida que la anticonfiabilidad disminuye.

En comparación RVR-AZVIS, en casi la totalidad de los casos RVR supera en performance a AZVIS por lo que es rotundamente más robusto para los casos donde la anticonfiabilidad de los grafos es alta. Esto puede tener diversos orígenes: lo que primero se le puede ocurrir al lector es que dadas las topologías y las probabilidades de operación la anticonfiabilidad no resulta ser un evento raro, y sabemos que por construcción AZVIS se desarrolla basándose en esta característica de los sistemas. Por otro lado, al ser una técnica iterativa para eventos raros en general frente a RVR una técnica recursiva desarrollada específicamente para la estimación de la anticonfiabilidad en redes, es natural pensar que la recursividad lo supere en performance. Además debemos tener en cuenta el enorme costo computacional de hallar los cortes de máxima probabilidad en cada paso iterativo de AZVIS. En cada iteración se calculan dos cortes: el del subgrafo G^-_{i+1} y el de G^+_{i+1}. Frente a RVR que simplemente necesita hallar un corte sin características especiales del grafo. Aún así con esta desventaja computacional AZVIS logra en los casos donde la anticonfiabilidad se aproxima a 0, resultados equivalentes en términos de varianza y esfuerzo computacional con respecto a RVR, y hasta logra superarlo en algunos casos. Por lo que a priori no debemos descartar que en contextos donde la anticonfiabilidad tienda realmente a cero AZVIS aumente en robustez y alcance a superar a RVR, mientras que RVR lo supere ampliamente en contextos inversos.

4

Bibliografía

[1] Michael O. Ball. Computational complexity of network reliability analysis: An overview. *IEEE Transactions on Reliability*, 35(3):230 –239, aug. 1986.

[2] B. Bollobás. *Random Graphs*. Cambridge University Press, 2001.

[3] E. Canale, H. Cancela, J. Piecini, F. Robledo, P. Romero, G. Rubino, and P. Sartor. Recursive variance reduction method in stochastic monotone binary systems. In *Reliable Networks Design and Modeling (RNDM), 2015 7th International Workshop on*, pages 135–141, Oct 2015.

[4] H. Cancela and M. El Khadiri. A recursive variance-reduction algorithm for estimating communication-network reliability. *IEEE Transactions on Reliability*, 44(4):595–602, 1995.

[5] Héctor Cancela and Mohamed El Khadiri. The recursive variance-reduction simulation algorithm for network reliability evaluation. *IEEE Transactions on Reliability*, 52(2):207–212, 2003.

[6] Charles J. Colbourn. Reliability issues in telecommunications network planning. In *Telecommunications network planning, chapter 9*, pages 135–146. Kluwer Academic Publishers, 1999.

[7] Stephen A. Cook. The complexity of theorem-proving procedures. In *Proceedings of the third annual ACM symposium on Theory of computing*, pages 151–158, New York, NY, USA, 1971. ACM.

[8] R.K. Dash, N.K. Barpanda, P.K. Tripathy, and C.R. Tripathy. Network reliability optimization problem of interconnection network under node-edge failure model. *Applied Soft Computing*, 12(8):2322 – 2328, 2012.

[9] George S. Fishman. A Monte Carlo sampling plan for estimating network reliability. *Operations Research*, 34(4):581–594, 1986.

[10] Michael R. Garey and David S. Johnson. *Computers and Intractability: A Guide to the Theory of NP-Completeness*. W. H. Freeman and Company, New York, NY, USA, 1979.

[11] Ilya B. Gertsbakh and Yoseph Shpungin. *Models of Network Reliability: Analysis, Combinatorics, and Monte Carlo*. CRC Press, Inc., Boca Raton, FL, USA, 1st edition, 2009.

[12] R. M. Karp. Reducibility among combinatorial problems. In R. E. Miller and J. W. Thatcher, editors, *Complexity of Computer Computations*, pages 85–103. Plenum Press, 1972.

[13] Pierre L'Ecuyer, Gerardo Rubino, Samira Saggadi, and Bruno Tuffin. Approximate zero-variance importance sampling for static network reliability estimation. *IEEE Transactions on Reliability*, 60(3):590–604, 2011.

[14] L. Petingi and J. Rodriguez. Reliability of networks with delay constraints. In *Congressus Numerantium*, volume 152, pages 117–12, 2001.

[15] A. Rosenthal. Computing the reliability of complex networks. *SIAM Journal on Applied Mathematics*, 32(2):384–393, 1977.

[16] G. Rubino and B. Tuffin. *Rare event simulation using Monte Carlo methods*. Wiley, 2009.

[17] A. Satyanarayana and Mark K. Chang. Network reliability and the factoring theorem. *Networks*, 13(1):107–120, 1983.