EFECTOS DE ATAQUE EN LA VULNERABILIDAD DE UN SISTEMA MODELADO A TRAVÉS DE REDES

Ing. Oscar Bastidas Pavlovitz

Trabajo de Grado presentado ante la ilustre

Universidad Central de Venezuela

para optar al título de

Magister Scientiarum en Investigación de Operaciones.

Caracas, Junio de 2006

DEDICATORIA:

A mi esposa, hijas, por su comprensión y apoyo durante los años que le dediqué a esta nueva meta.

A mis padres, quienes me infundieron la ética y perseverancia que me orientan transitar por la vida.

AGRADECIMIENTOS:

Al Profesor Claudio Rocco, quien con su paciencia y perseverancia dedicó su tiempo para el logro de esta nueva meta…., A Ud. Profesor, el mayor de mis agradecimientos.

Al Ingeniero Andrés Díaz, por su por su predisposición permanente e incondicional apoyo y por sus constantes y substanciales sugerencias, por su amistad.

RESUMEN

En este Trabajo Especial se desarrollan varios modelos matemáticos que permiten evaluar el comportamiento de una red ante un posible ataque. Los modelos pueden ser utilizados para determinar el daño que un ataque ocasiona en el funcionamiento de un sistema y sugerir esquemas de protección para hacerlos más resistentes a la interrupción.

El presente trabajo emprende el desarrollo de modelos en sistemas que están representados como un conjunto de nodos interconectados por enlaces. En la primera parte se plantea la problemática a estudiar: el ataque se realiza en un nodo de la red y como éste se propaga a través del sistema. Se proponen dos tipos de evaluaciones: 1) determinar el tiempo mínimo que tarda el ataque en propagarse desde un nodo inicial hasta un nodo destino y 2) determinar el tiempo mínimo que tarda un ataque en alcanzar todos los nodos. Estas situaciones son evaluadas a través de algoritmos de caminos mínimos y árboles de expansión mínimos.

Posteriormente, se determina cómo evoluciona en el tiempo la propagación del ataque y qué efectos se producen en el sistema. Para esto se propone un modelo sencillo basado en la determinación del número de personas afectadas en cada nodo que es atacado. Esta evaluación se realiza a través de un enfoque basado en Autómatas Celulares.

Se proponen modelos que consideran la aleatoriedad en los tiempos de propagación del ataque y en la cantidad de personas afectadas. Esta evaluación se realiza a través de Simulación Monte Carlo.

Por último se propone un modelo para minimizar el daño de un ataque, mediante la definición de un esquema de inmunización de los nodos.

ÍNDICE GENERAL.

ÍNDICE DE FIGURAS.

ÍNDICE DE TABLAS.

CAPÍTULO I

PRESENTACIÓN DEL PROBLEMA

1.1. INTRODUCCIÓN.

En este capítulo se presenta un estudio de la problemática propuesta así como aspectos generales que permitirán al lector una comprensión sencilla. Una vez descrito el problema en cuestión, se forman los objetivos generales como parte de las actividades a ampliar. Con base a éstos, se establece la importancia de este trabajo a través del alcance, posteriormente se constituye la metodología de trabajo.

1.2. ANTECEDENTES.

Nuestra sociedad y nuestro mundo moderno dependen de un sistema complejo compuesto de infraestructuras críticas. Por ejemplo, la "National Strategy for Homeland Security"[1] de Estados Unidos, ha identificado varios sectores críticos de amenazas, medios de ataque, que hacen blancos lucrativos para los terroristas. Dentro de estos sectores críticos tenemos a la agricultura y alimentación, agua, salud pública, servicios de emergencia, gobierno, información y telecomunicaciones, energía, transporte, actividades bancarias y financieras, productos químicos y materiales peligrosos, carga y correo, entre otros [SEC].

El incremento de los ataques y amenazas después del 11 de septiembre del 2001, coordinados con el atentado del 11 de Marzo del 2004 en Madrid, el atentado del 7 de julio del 2005 en Londres, entre otros, ha creado la necesidad de elevar los servicios de seguridad y las habilidades para prevenir futuros eventos [NIS]. Estas amenazas son diversas por su naturaleza, se extienden desde un ataque a un sistema de computación, que podría causar un derrumbamiento económico temporal, hasta el lanzamiento de bombas y armas biológicas en lugares claves.

Los gobiernos han fijado una agenda que abarca la legislación y el desarrollo de una serie de estrategias a largo plazo para prevenir estos ataques y que se construya alrededor de cuatro P´s: prevenir, perseguir, proteger y prepararse [BRA]. Una estrategia, representa una política clara de reducir el riesgo y el impacto de estos ataques.

Ahora, bien, valorar los riesgos de los sectores críticos [SEC], responde a las siguientes preguntas: ¿Qué tan malo puede ser?, ¿Cuáles son sus consecuencias?, ¿Cuán susceptible es un sistema a un ataque?. Evidentemente se requiere definir el concepto de daño: estos daños pueden ser cantidad de personas afectadas dentro de

[1] Estrategia Nacional para la Seguridad del País.

una red de distribución, por ejemplo, agua potable o el tiempo de propagación de un ataque [APO].

Siguiendo este orden de ideas, una red es la representación básica de un sistema interconectados por enlaces. Estos enlaces pueden estar expuestos a una interrupción indebida, causando daño y afectando el funcionamiento de la red.

En los últimos años, se han desarrollado modelos para la evaluación de la confiabilidad en sistemas representados a través de redes. Entre los criterios que se usan para cuantificar la confiabilidad, se encuentra el criterio de continuidad entre dos puntos de la red, "Two Terminal" o, el más amplio, la evaluación denominada "All-Terminal". Esta última busca determinar la probabilidad que exista continuidad entre cualesquiera puntos de la red [BIL] [COL].

En este Trabajo Especial se pretenden desarrollar algunos modelos matemáticos que permitan evaluar el posible comportamiento de una red ante un ataque, a través de una interpretación de los criterios de confiabilidad. Los modelos a desarrollar permitirán evaluar posibles esquemas de diseño así como acciones preventivas.

El tema de ataques a sistemas representados por redes ha sido estudiado anteriormente a través de modelos matemáticos que han permitido caracterizar algunos tipos de redes y proponer esquemas preventivos [BRA] [BOD] [ROC]. Los modelos a desarrollar en este Trabajo Especial, se diferencian de trabajos anteriores en dos aspectos principales: a) considerar el tiempo que le toma a un ataque en propagarse por la red y b) permitir cuantificar el efecto del ataque a través de la evaluación de las posibles personas afectadas en cada punto de la red.

1.3. PLANTEAMIENTO DEL PROBLEMA.

Se tiene un sistema que puede ser representado a través de una red (por ejemplo: una red de distribución de agua) y una posible acción de ataque (por ejemplo la colocación de un agente venenoso en la red) [ZIO].

El sistema está representado como un conjunto de nodos interconectados por enlaces. El ataque se realiza en un nodo de la red y tan pronto el ataque es completado, su efecto dañino comienza a propagarse a través del sistema. Por ejemplo, en la red de la figura 1.1, se inicia un ataque en el nodo 10. Los efectos de este ataque se propagan a los nodos 1, 4, 6 y 8.

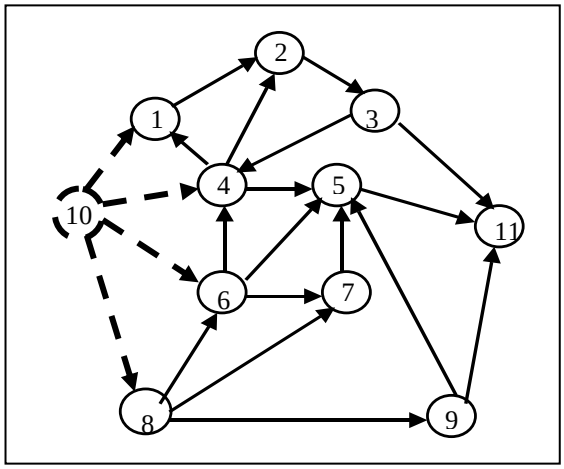


Figura 1.1: Red de 11 nodos y 21 enlaces.

Una vez que se concreta el ataque, se pretenden desarrollar dos modelos básicos, inspirados en la evaluación de la confiabilidad[2] de una red, que permitan los siguientes análisis:

[2] Confiabilidad de una red. - Es una medida que refleja la capacidad de la misma de continuar operativa frente a posibles fallos de algunos de sus componentes, y se define como la probabilidad de comunicación entre un nodo de origen "S" a un nodo de destino "D", dadas las probabilidades de funcionamiento de los componentes y la topología de la red.

a) Evaluar el tiempo que tardan los efectos del ataque en alcanzar un nodo específico (por ejemplo el nodo 11 en la figura 1). Este modelo es una extensión del criterio de continuidad, también llamado “Two Terminal”.

b) Evaluar el tiempo que tardan los efectos del ataque en alcanzar todos los nodos. Este modelo es una extensión del criterio de “All Terminal”.

Estos modelos básicos pueden extenderse para considerar aspectos estocásticos (por ejemplo, modelar tiempos de propagación aleatorios entre nodos) o para evaluar los efectos del ataque (por ejemplo, considerando el número de personas o usuarios de la red que son afectados en cada nodo) [ROC].

La definición de los modelos a) y b), permiten posteriormente analizar, por ejemplo, el efecto de ataques en diferentes nodos o el efecto de alguna política de prevención. Por ejemplo, cómo se modifica el tiempo de propagación en el modelo a), si se elimina una conexión.

Para el análisis del problema a), el estudio se desarrolla a través del algoritmo Dijkstra, el cual tiene por objetivo encontrar la ruta mas corta (la trayectoria con la mínima distancia[3] total) que va desde el origen al destino.

Para el análisis del problema b), el estudio se desarrolló a través del algoritmo del árbol de expansión que consiste en encontrar los enlaces más cortos entre todos los nodos de la red. El problema elige los enlaces en la red que tengan la distancia total más corta al mismo tiempo que proporciona una trayectoria entre cada par de nodos.

En este trabajo se considera como vulnerabilidad, la propiedad de la red en soportar amenazas y peligros limitando su capacidad de funcionamiento [HOL], cuando ésta es atacada bien sea bajo el caso a) o el caso b).

[3] Esta distancia puede ser también tiempo, costo o alguna cantidad.

El estudio de vulnerabilidad de una red, por ejemplo nodos, permite identificar puntos críticos en un sistema, en los que posibles ataques incrementan considerablemente el número de personas afectadas o causan que la propagación del ataque se manifieste más rápidamente.

1.4. DEFINICIÓN DE OBJETIVOS.

GENERAL:

Desarrollar modelos matemáticos que permitan determinar la vulnerabilidad de una red expuesta a un ataque.

ESPECÍFICOS:

- Definir dos modelos elementales basados en los dos criterios mas usados en la evaluación de la confiabilidad ("Two Terminal" y "All Terminal") que permitan obtener el tiempo de propagación de un ataque a través de la red y el promedio de personas afectadas.

- Modelar aspectos estocásticos básicos a través de Simulación Monte Carlo, tales como: tiempo de propagación entre nodos y número de personas afectadas que permiten el análisis para tomar acciones preventivas.

- Estudiar las técnicas de evaluación en redes, tales como modelos de Dijkstra o Árbol de Expansión[4].

- Estudiar los efectos de posibles acciones de protección previas al ataque para minimizar las consecuencias.

[4] Spanning Tree.

1.5. METODOLOGÍA DE LA INVESTIGACIÓN.

La metodología planteada para desarrollar el objetivo general incluye una investigación de tipo documental así como actividades experimentales. Dentro de las actividades pautadas se puede mencionar:

- Revisión Bibliográfica acerca de trabajos anteriores y conceptos básicos para relacionarlos al ámbito de estudio aplicable a esta investigación.
- Establecimiento de métodos de cálculo de redes para verificar la funcionalidad de los problemas planteados.
- Redactar el trabajo final como una herramienta de fácil utilización dentro del campo de aplicación.

1.6. ORGANIZACIÓN DEL TRABAJO.

El contenido de este trabajo se ha estructurado en cuatro capítulos, donde:

Capítulo I, plantea la problemática a estudiar, descripción del objetivo general y objetivos específicos así como la metodología implementada para el desarrollo de este estudio.

Capítulo II, contiene en forma breve la terminología básica sobre redes así como el desarrollo de dos algoritmos, Dijkstra y el Árbol de Expansión Mínimo para la evaluación del modelo de la ruta más corta.

Capítulo III, presenta la evaluación del tiempo de propagación de un ataque combinando la metodología Autómata Celular y la interpretación de dos modelos básicos de confiabilidad: “Two Terminal” y “All Terminal”.

Capítulo IV, señala un ejemplo aplicando los modelos “Two Terminal” y “All Terminal”. En él se determina el tiempo de propagación del ataque y el número de personas afectadas cuando a) el ataque alcanza un nodo de destino y b) cuando el ataque alcanza todos los nodos de la red.

Finalmente se recogen las conclusiones y recomendaciones a las cuales conlleva este trabajo.

CAPÍTULO II

ASPECTOS TEÓRICOS DE REDES

2.1. INTRODUCCIÓN

En este capítulo se presentan las definiciones básicas sobre la terminología de redes que serán usadas en este trabajo, así como el desarrollo de dos modelos para la evaluación de la ruta más corta entre dos puntos, (a través del Algoritmo de Dijkstra) y la determinación del Árbol de Expansión Mínimo.

2.2. REDES

Los sistemas modelados como redes surgen en una gran variedad de situaciones. Las redes de transporte, eléctricas y de comunicaciones predominan en nuestra vida diaria. La representación de redes se utiliza ampliamente en áreas tan diversas como producción, distribución, planificación de proyectos, localización de instalaciones, administración de recursos y planificación financiera de proyectos, por nombrar algunos cuantos ejemplos. De hecho, una representación de redes proporciona un panorama general tan poderoso y una ayuda conceptual para visualizar las relaciones entre los componentes de los sistemas que se usa casi en todas las áreas científicas, sociales, económicas [MER] [REK]. Cabe destacar, que estos modelos de redes siempre están orientados a optimizar situaciones reales. La tabla II.1 proporciona varios ejemplos de representación de redes.

Tabla II.1. Componentes de redes representativas.

Nodos	**Enlaces**
Cruceros	Caminos
Aeropuertos	Líneas Aéreas
Puntos de Conmutación	Cables, canales.
Estaciones de Bombeo	Tuberías
Centros de Trabajo	Rutas de manejo de materiales

Es importante destacar, que las redes se emplean en distintas disciplinas para modelar relaciones entre objetos: los objetos se representan por nodos de la red, y dos objetos están conectados por un enlace si están relacionados entre sí.

Una red consiste en un conjunto de puntos y un conjunto de líneas que unen cierto pares de puntos. Los puntos se llaman *nodos* o vértices. Por ejemplo, en la figura 2.1., la red consta de 5 nodos. Las líneas se llaman enlaces (arcos, aristas, ligaduras o ramas). Por ejemplo, en la figura 2.1., la red consta de 8 enlaces. Los enlaces se etiquetan dando

nombre a sus nodos en sus puntos terminales. Siguiendo con la figura 2.1., *(1, 2)* es el enlace entre los nodos *1* y *2* [TAJ] [AHO] [HIL].

La notación estándar para describir una red es *G = (N, E)*, donde *N* es el conjunto de nodos y *E* es el conjunto de enlaces. En la figura 2.1 se describe una representación gráfica de una red de 5 nodos y 8 enlaces.

N = (1,2,3,4,5) E = {(1,5), (1,2), (2,5), (5,4), (3,4), (3,2), (2,3), (4,5)}

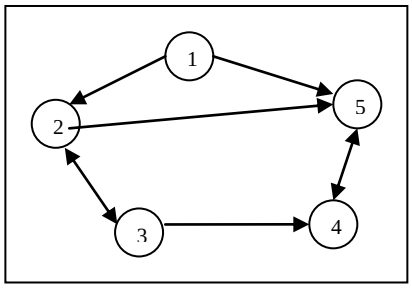


Figura 2.1. Representación gráfica de una red *G = (N, E)*.

Cada nodo puede establecer enlaces (vínculos, relaciones) con otros nodos. Estos enlaces representan flujo, tiempo, costos, entre otras variables, y están limitados por su capacidad[1]. A su vez, estos enlaces pueden estar orientados o dirigidos y no dirigidos.

Los enlaces de una red pueden tener un flujo de algún tipo que pasa por ellos, por ejemplo, el flujo de automóviles sobre los caminos de una ciudad. Si el flujo a través de un enlace se permite sólo en una dirección (como en una calle de un sentido), se dice que el enlace es un *enlace dirigido*. Al etiquetar un enlace con el nombre de los nodos que los une, siempre se pone primero el nodo de *donde viene* y después el nodo a *donde va*, esto es, un enlace dirigido del nodo *1* al nodo *2* debe etiquetarse como *(1, 2)* y no como *(2, 1)*, otra manera de etiquetarlo es *1* → *2*.

[1] En el presente estudio, el enlace esta representado por el tiempo de propagación del ataque.

Si el flujo a través de un enlace se permite en ambas direcciones como en calles de dos sentidos), se dice que el enlace es un *enlace no dirigido*, por ejemplo, el la figura 2.1, el enlace no dirigido es (*2, 3)* = (3, *2).*

Una red que solo tiene enlaces dirigidos se llama red dirigida, de igual manera, si todos sus enlaces son *no dirigidos*[2], se dice que se trata de una *red no dirigida*. Una red con una mezcla de enlaces dirigidos y no dirigidos se puede convertir en una red dirigida, sustituyendo cada enlace no dirigido por un par de enlaces dirigidos en direcciones opuestas [AHO].

Una trayectoria es una secuencia de enlaces distintos que conectan dos nodos sin considerar la orientación de los enlaces individuales. Por ejemplo, una de las trayectorias que conectan a los nodos de 1 al 5 de la figura 2.1, es la sucesión de enlaces (1, 2) – (2, 5) ó (1→ 2→ 5). Cuando algunos o todos los enlaces de una red son enlaces dirigidos, se hace la distinción entre las trayectorias dirigidas y no dirigidas. Una *trayectoria dirigida* del nodo *i* al nodo *j*, es una sucesión de enlaces cuya dirección es hacia el nodo *j*, de manera que el flujo del nodo *i* al nodo *j* a través de la trayectoria sea factible. Una *trayectoria no dirigida* del nodo *i* al nodo *j* es una sucesión de enlaces cuya dirección puede ser hacia o desde el nodo *j* [HIL].

2.3. ALGORITMO DE DIJKSTRA [AHO] [HIL] [TAJ] [WIK].

El Algoritmo de Dijkstra encuentra la distancia más corta entre un nodo origen *S*[3] y un nodo destino *D*[4]. Cabe destacar que este algoritmo posee numerosas e importantes aplicaciones, que hacen de él uno de los más relevantes en la teoría de redes. Por ejemplo: enrutamiento de paquetes de una red telefónica, enrutamiento de aviones y tráfico aéreo, entre otros.

[2] En éste estudio, el tiempo de propagación del ataque del nodo 1 al nodo 2 es igual al tiempo de propagación del ataque del nodo 2 al nodo 1.
[3] *S* se denominará como nodo de origen y proviene del inglés “Source”.
[4] *D* se denominará como nodo de destino y proviene del inglés “Destination”.

Se supone una red dirigida *G = (N, E)*, en el cual cada enlace tiene una etiqueta no negativa[5], y donde un nodo se especifica como origen. El problema[6] es determinar el camino más corto desde el origen *S* a un destino *D*, donde la longitud del camino es la suma de los valores de los enlaces del camino.

Por ejemplo, sea una red *G* un mapa de vuelos en el cual cada nodo representa una ciudad, y cada enlace $i \rightarrow j$, una ruta aérea de la ciudad *i* a la ciudad *j*. La etiqueta del enlace $i \rightarrow j$ es el tiempo que se requiere para volar de *i* a *j*. La solución del problema de los caminos más cortos partiendo desde el origen determinará el tiempo de viaje mínimo para ir de cierta ciudad a otra ciudad del mapa. Para resolver este problema se utilizará el algoritmo de Dijkstra.

El algoritmo Dijkstra opera a partir de un conjunto *S* de nodos cuya distancia más corta desde el origen ya es conocida. En principio *S* contiene solo el nodo de origen. En cada paso se agrega algún nodo restante *i* a *S*, cuya distancia desde el origen es la más corta posible. Suponiendo que todos los enlaces tienen un valor no negativo, siempre es posible encontrar un camino más corto entre el origen e *i* que pasa sólo a través de los nodos de *S* y que se llama *elegido*. En cada paso del algoritmo se usa un vector *D* para registrar la longitud del camino *elegido* más corto a cada nodo. Una vez que *S* incluye todos los nodos, todos los caminos son *elegidos*, así que *D* contendrá la distancia más corta del origen a cada nodo.

2.3.1. Descripción Detallada del Algoritmo.

Entrada: Un red conexa[7] con todos sus enlaces positivos, y los nodos inicial y final del camino.

[5] Valores Positivos.
[6] En el presente estudio, se buscará el menor tiempo desde el origen *S* al destino *D.*
[7] Red conexa: si todos sus nodos están conectados por un camino; es decir, si para cualquier par de nodos (a, b), existe al menos un camino posible desde *a* hacia *b*. Se debe resaltar que no es necesario que la trayectoria sea dirigida aún cuando la red sea dirigida.

Salida: La longitud de la ruta más corta entre esos nodos de la red.

- Sea *G=(N,E)* una red dirigida y etiquetada.
- Sean los nodos $i \in N$ y $j \in N$; *i* es el nodo de origen y *j* el nodo de destino.
- Sea un conjunto $S \in N$, que contiene los nodos de *N* cuyo camino más corto desde *a* todavía no se conoce.
- Sea un vector *D*, con tantas dimensiones como elementos tiene *N*, y que guarda las distancias entre *a* y cada uno de los nodos de *N*.
- Sea, finalmente, otro vector *P*, con las mismas dimensiones que *D*, y que conserva la información sobre qué nodo precede a cada uno de los nodos en el camino.

Pasos

1. $S \leftarrow N$
2. Para todo nodo $i \in S$, $i \neq a$, se establece $D_i \leftarrow \infty$; $D_a \leftarrow 0$
3. Para todo nodo $i \in S$ se establece $P_i = a$
4. Se obtiene el nodo $s \in C$ tal que no existe otro nodo $z \in S$ tal que $D_z < D_s$
    - Si $s = z$ entonces se ha terminado el algoritmo.
5. Se elimina de S el nodo *s*: $S \leftarrow S - \{s\}$
6. Para cada enlace $e \in E$ de longitud *l*, que une el nodo *s* con algún otro nodo $t \in S$,
    - Si $l + D_s < D_t$, entonces:
        1. Se establece $D_t \leftarrow l + D_s$
        2. Se establece $P_t \leftarrow s$
7. Se regresa al paso 4

Al terminar este algoritmo, en D_z estará guardada la distancia mínima entre *a* y *z*. Por otro lado, mediante el vector *P* se puede obtener el camino mínimo: en P_z estará *y*, el nodo que precede a *z* en el camino mínimo; en P_z estará el que precede a *y*, y así sucesivamente, hasta llegar a *a*.

Para ilustrar este procedimiento, se considera la red de la Figura 2.2. Los números en cada enlace representan el tiempo de propagación entre sus nodos, en unidades arbitrarias. Por ejemplo, cuando el nodo 1 es activado por un "ataque", activará al nodo 2 después de 2 unidades de tiempo y al nodo 3 después de 3 unidades de tiempo.

Dado un "ataque" inicial en el nodo 1, el problema consiste en determinar el camino más corto hasta el nodo de destino 6, esto es el tiempo mínimo que tarda el ataque en propagarse desde el nodo 1 al nodo 6.

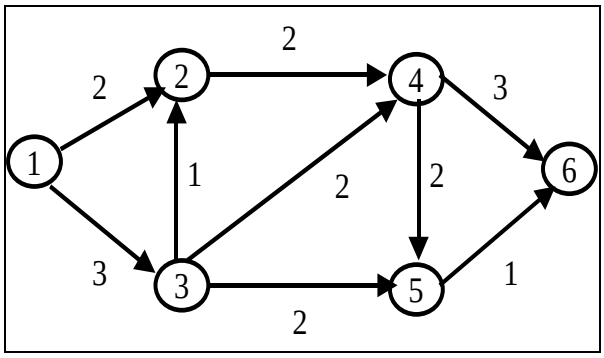


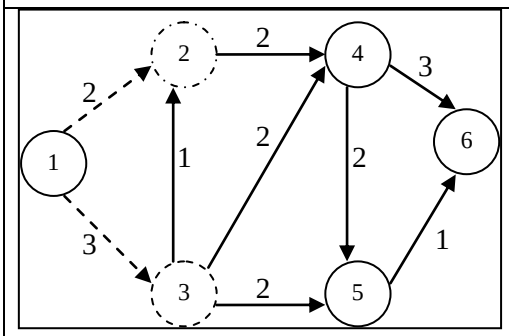
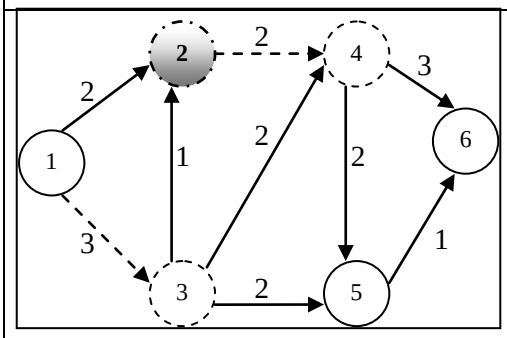
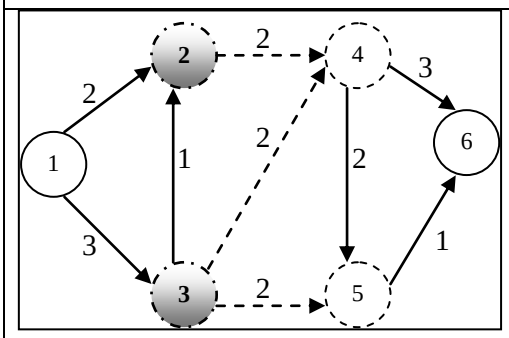
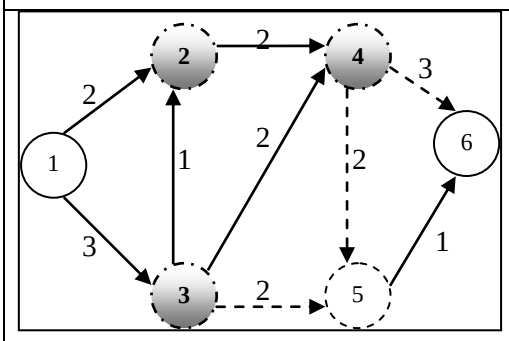
Figura 2.2. Representación gráfica de una red cuyos enlaces representan el tiempo entre cada nodo.

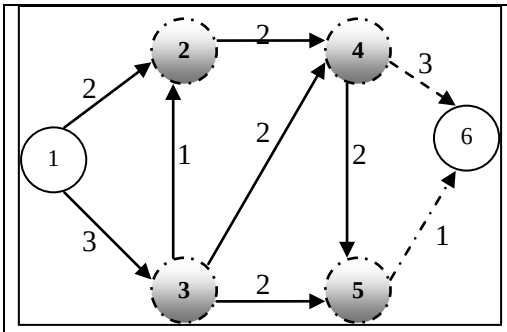
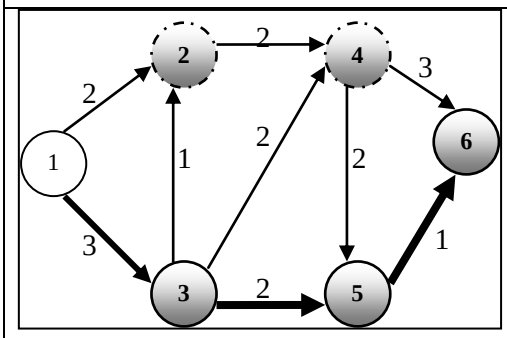
El resultado de la aplicación de este algoritmo se muestra a continuación. La tabla II.2 presenta la secuencia de los valores de *D* después de cada iteración, mientras que la tabla II.3 detalla la evolución del algoritmo.

Tabla II.2 Resultados de Dijkstra de la red dirigida de la figura 2.2.

Paso	***S***	***P***	***D[2]***	***D[3]***	***D[4]***	***D[5]***	***D[6]***
Inicio	{1}	--	2	3	∞	∞	∞
1	{1,2}	2	2	3	4	∞	∞
2	{1,2,3}	3	2	3	4	5	∞
3	{1,2,3,4}	4	2	3	4	5	7
4	{1,2,3,4,5}	5	2	3	4	5	6
5	{1,2,3,4,5,6}	6	2	3	4	5	6

Tabla II.3 Descripción paso a paso del algoritmo Dijkstra.

Representación Gráfica	Paso	Descripción
	Inicio	Los enlaces entrecortados apuntan a nodos alcanzables desde el nodo inicial. El tiempo a: D[2] =2, D[3] =3. El nodo 2 tiene el menor tiempo. Cualquier otro camino a 2 pasa por otros nodos de la red, será más largo que 2.
	1	Los enlaces entrecortados apuntan a nodos alcanzables desde nodos que ya tienen un tiempo establecido. El tiempo a: D[3] =3, D[4] = 4. El nodo 3 tiene el menor tiempo. No hay otros enlaces entrando a 3. El nodo 3 será demarcado para indicar que 3 es el tiempo más corto al nodo 3.
	2	Los enlaces entrecortados apuntan a nodos alcanzables desde nodos que ya tienen un tiempo establecido. El tiempo a: D[5] = 5, D[4] = 4. El nodo 4 tiene el menor tiempo. No hay otros enlaces entrando al nodo 4. El nodo 4 será demarcado para indicar que 4 es el tiempo de demora más corto al nodo 4.
	3	Los enlaces entrecortados apuntan a nodos alcanzables desde nodos que ya tienen un tiempo establecido. La distancia a: D[5] = 5, D[6] = 7. El nodo 5 tiene la distancia mínima. No hay otros enlaces entrando a 5. El nodo 5 será demarcado para indicar que 5 es el tiempo más corto al nodo 5.

	4	Los enlaces entrecortados apuntan a nodos alcanzables desde nodos que ya tienen un tiempo establecido. La distancia a: D[6] = 6. No hay otros enlaces entrando a nodo 6. El nodo 6 será demarcado para indicar que 6 es el tiempo más corto al nodo 6.
	5	El algoritmo ha terminado, siga las aristas demarcadas desde el nodo inicial a cualquier nodo para obtener el tiempo más corto al nodo 6, el cual se obtuvo 6 unidades. El tiempo de demora más corto se remarca en la figura izquierda.

2.4. ALGORITMO DEL ÁRBOL DE EXPANSIÓN MÍNIMO. ("MINIMUM SPANNING TREE")

El problema del árbol de expansión mínima tiene algunas similitudes con el problema de la ruta más corta presentada en la sección 2.3, en este caso, se considerará una red no dirigida, en la que la información incluye los nodos y los pesos[8] de los enlaces entre los pares de nodos. La diferencia para el problema del árbol de expansión mínima es que, en lugar de encontrar la ruta más corta a través de una red completamente definida, el problema elige los enlaces en la red que tengan la longitud total más corta y al mismo tiempo que proporcionan una trayectoria entre cada par de nodos. Es necesario que los enlaces se elijan de tal manera que la red resultante forme un árbol que se expande (conecta) a través de todos los nodos dados. En resumen, el problema es encontrar el árbol de expansión con la longitud total mínima de sus enlaces [TAJ] [MOS].

Una aplicación típica de los árboles de expansión mínimo tiene lugar en el diseño de redes de comunicación. Los nodos de la red representan las ciudades, y los enlaces, las posibles líneas de comunicación entre ellas [HER] [CAM]. El costo asociado a un enlace representa el costo de seleccionar esa conexión. Por ejemplo, un árbol de expansión mínimo representa una red que comunica todas las ciudades a un costo mínimo. Otros ejemplos en los que surge una decisión parecida incluyen la planificación de redes de transporte, redes de distribución.

Dado una red $G = (N, E)$, conexa donde cada enlace (i,j) de E tiene un costo asociado $C (i, j)$. Un árbol T de expansión para G es un árbol que conecta todo los nodos de N; su costo es la suma de todos los pesos de los enlaces del árbol.

[8] Pesos de los enlaces, son unidades de tiempo, costo, longitud, etc. Para este estudio, el peso estará representado por unidades de tiempo.

El algoritmo del árbol de expansión mínima necesita comenzar con cualquier nodo y conectar éste con el nodo más cercano. Los dos nodos resultantes forman un conjunto conectado de *S* y los nodos restantes constituyen el conjunto no conectado de $\overline{S}$.

Uno de los métodos de construcción de un árbol de expansión es el algoritmo de PRIM[9], que se define como un *algoritmo* que encuentra un subconjunto de enlaces que forman un árbol con todos sus nodos, en donde el tiempo total de todos los enlaces en el árbol de expansión es el mínimo posible.

2.4.1. Descripción Detallada del Algoritmo PRIM [AHO] [WIK] [HIL].

El algoritmo de PRIM, es un algoritmo de la teoría de redes para encontrar un árbol de expansión mínimo de una red conectada y cada enlace con un valor de costo. Este algoritmo encuentra un subconjunto de enlaces que forman un árbol con todos los nodos, en donde el peso total de los enlaces en el árbol es el mínimo posible. Si la red no está conectada, entonces el algoritmo encontrará el árbol de expansión mínimo para uno de los componentes conectados.

La idea básica consiste en añadir en cada paso un enlace de peso mínimo a un árbol previamente construido. Es decir:

1. Se crea un árbol con un solo nodo, elegido al azar.

2. Se crea un conjunto con todos los enlaces.

3. Repetir hasta que cada enlace en el conjunto conecte dos nodos del árbol.

    3.1. Eliminar del conjunto el enlace con mínimo peso que conecte un nodo en el árbol con un nodo fuera del árbol.

[9] El algoritmo fue diseñado en 1930 por el matemático Vojtech Jarnik y luego de manera independiente por el científico computacional Robert C. Prim en 1957 y redescubierto por Dijkstra en 1959. Por esta razón el algoritmo es también conocido como *algoritmo DJP* o *algoritmo de Jarnik.*

3.2. Añadir este enlace al árbol.

Para ilustrar este procedimiento, se considera la red de la Figura 2.3. Los números en cada enlace, representan por ejemplo, el tiempo de propagación entre sus nodos, en unidades arbitrarias. El nodo 1 es activado por un ataque; se busca determinar cuál es el tiempo total de propagación del ataque por toda la red.

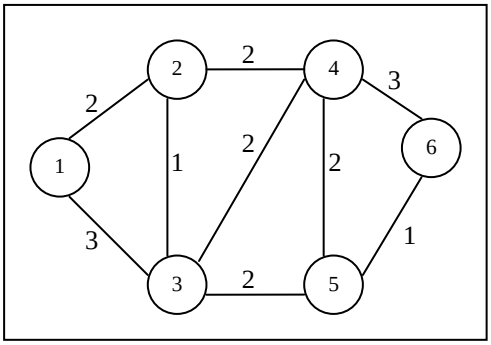
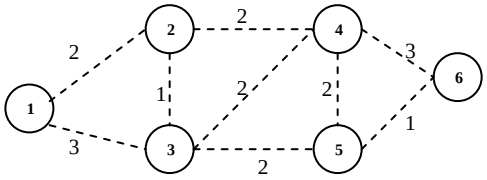
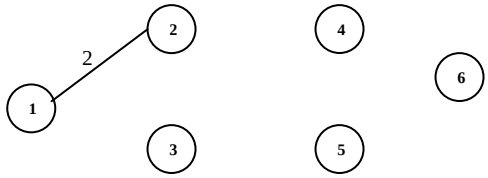
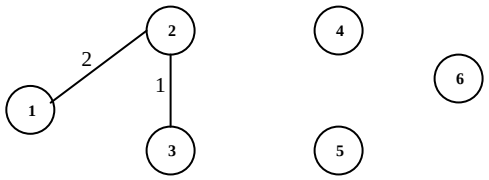
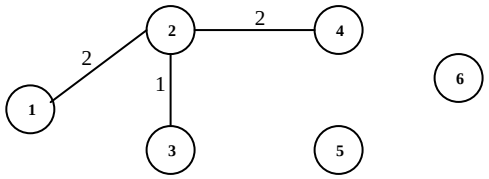
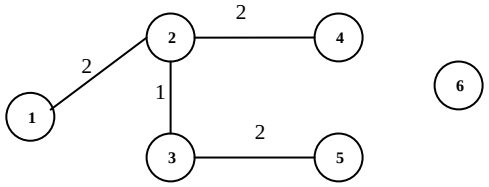


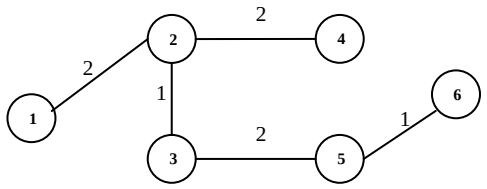
Figura 2.3. Representación gráfica de una red no dirigida cuyos enlaces representan el tiempo de propagación del ataque entre cada nodo.

En la Tabla II.4 se muestra la evolución detallada del algoritmo de PRIM.

Tabla II.4. Descripción paso a paso del algoritmo PRIM.

Inicio	$S = 0$, $\bar{S} = 1,2,3,4,5,6$	
Los números cerca de los enlaces indican el tiempo de propagación, que viene siendo el peso de cada enlace. Todos los enlaces están con líneas entrecortadas y el nodo 1 ha sido elegido como punto de partida, es decir, el nodo donde el ataque es perpetrado.		

<table>
<tr><td>1</td><td>$S = \{1\}$;
$\overline{S} = \{2,3,4,5,6\}$</td><td> 
</td></tr>
<tr><td colspan="3">El nodo más cercano a 1 es el nodo 2, con un tiempo de 2 unidades, el nodo 3, con un tiempo de 3 unidades. De éstos, el nodo 2 es el valor más bajo, así que se demarca el enlace 1 – 2.</td></tr>
<tr><td>2</td><td>$S = \{1,2\}$; $\overline{S} = \{3,4,5,6\}$;
T = {1–2}</td><td> 
</td></tr>
<tr><td colspan="3">El siguiente nodo elegido es el nodo más cercano a cualquiera de los nodos del árbol construido. En este caso, el nodo 3 se encuentra a un tiempo de 1 unidad del nodo 2 y a un tiempo 3 unidades del nodo 1, así que se demarca el enlace 2-3.</td></tr>
<tr><td>3</td><td>$S = \{1,2,3\}$; $\overline{S} = \{4,5,6\}$;
T = {1–2, 2-3}</td><td> 
</td></tr>
<tr><td colspan="3">El nodo 4, que está a un tiempo de 2 unidades del nodo 2, a un tiempo de 4 unidades del nodo 1 y a un tiempo de 5 unidades del nodo 1 a través del nodo 3, así que se demarca el enlace 2 – 4, el cual posee el menor tiempo de propagación.</td></tr>
<tr><td>4</td><td>$S = \{1,2,3,4\}$, $\overline{S} = \{5,6\}$,
T = {1–2, 2-3, 2-4}</td><td> 
</td></tr>
<tr><td colspan="3">El nodo más próximo al árbol construido es el 5, que se encuentra con un tiempo de 2 unidades del nodo 3 o a 5 unidades desde el nodo 1 a través del nodo 3 y a un tiempo de 6 unidades a través del nodo 4, por lo tanto, se demarca el enlace 3 – 5, que posee el valor más bajo.</td></tr>
</table>

5	$S = \{1,2,3,4,5\}$; $\bar{S} = \{6\}$; T = {1-2, 2-3, 2-4, 3-5}	
El nodo más próximo al árbol construido es el 6, que se encuentra con un tiempo de 1 unidad del nodo 5 o de 6 unidades desde el nodo 1 a través del nodo 3 - 5 y a un tiempo de 7 unidades a través de los nodos 1 – 2 - 4, por lo tanto, se demarca el enlace 5 – 6, que posee el valor más bajo.		
6	$S = \{1,2,3,4,5,6\} = P$; $\bar{S} = 0$; T = {1-2, 2-3, 2-4, 3-5, 5-6}	T = 2 + 1 + 2 + 2 + 1 = 8
Todos los nodos quedaron conectados, por un tiempo de 8 unidades.		

Es importante resaltar que el tiempo que se obtiene mediante el uso de este algoritmo no necesariamente corresponde al tiempo mínimo de propagación ya que este fenómeno puede darse en "paralelo". Por ejemplo, en la red de las figuras de la tabla II.4, el nodo 4 es activado en un tiempo t = 4 unidades, y el nodo 3 en un tiempo t = 3 unidades. Sin embargo, entre el tiempo t = 3 unidades y el tiempo t = 4 unidades, el efecto del ataque se está propagando desde el nodo 3 hacia el nodo 5 y posteriormente hasta el nodo 6, el tiempo total para alcanzar todos los nodos es de 6 unidades.

En el próximo capítulo, se analiza esta situación y se propone una solución basada en el enfoque de autómata celular.

CAPÍTULO III

MODELOS DE ATAQUE

3.1. INTRODUCCIÓN.

Este capítulo presenta dos modelos para la evaluación del tiempo de propagación de un "ataque" combinando los algoritmos Dijkstra y Árbol de Expansión Mínima con la metodología Autómata Celular y la interpretación de los dos modelos básicos de confiabilidad: "Two Terminal" y "All Terminal".

3.2. AUTÓMATA CELULAR [ROC].

Los algoritmos Dijkstra y Árbol de Expansión Mínimo, permiten determinar el tiempo de propagación para los problemas:

a) Evaluación del tiempo en el que el "ataque", alcanza un nodo de destino ***i*** ($TTRD_i$)[1].

b) Evaluación del tiempo en el que el "ataque", alcanza todos los nodos de la red. (TTRAD)[2].

Sin embargo, estas evaluaciones no proporcionan información de cómo evoluciona en el tiempo la propagación del ataque. Esta información es importante si se quiere modelar los efectos que se suceden en cada iteración como, por ejemplo, el número de personas afectadas en cada nodo que es alcanzado por el ataque. Esta información se puede obtener utilizando el enfoque basado en Autómatas Celulares, tal y como se muestra en esta sección.

Un Autómata Celular (AC), es un sistema dinámico discreto que está compuesto por un conjunto de células, celdas, entes o agentes, cada uno de ellos susceptible de encontrarse en un cierto estado y de cambiarlo de un instante al siguiente, suponiendo que el tiempo transcurre de forma discreta.

La regla que gobierna la transición de estados en los entes es sensible a los estados de los demás elementos en su vecindad, siendo por tanto una regla de transición "*local*". El aspecto que más caracteriza a los Autómatas Celulares es su capacidad para dotar al conjunto del sistema, visto globalmente, de una serie de propiedades emergentes inducidas por la propia dinámica local.

[1] TTRD – Total Time to Reach Destination.
[2] TTRAD – Total Time to Reach All Destination.

La definición de un AC requiere fijar los siguientes puntos:

Conjunto de células. Se necesita saber cuántos objetos elementales van a formar la población del sistema. En principio no hay restricción a su número, pudiendo ser desde unos pocos hasta una infinidad numerable. En ocasiones es importante situarlos sobre una región geográfica, identificándose entonces los entes con sus respectivas coordenadas geográficas.

Vecindades. Para cada elemento del sistema es necesario establecer su vecindad: aquellos otros elementos que serán considerados como sus vecinos. En caso de asociar objetos con coordenadas de un sistema de referencia, el criterio suele ser construir la vecindad de un elemento dado con todos aquellos otros elementos que se encuentran a menos de una cierta distancia o radio, de forma que los más alejados no ejerzan influencia directa sobre él.

En el caso de una dimensión, dispuestas las células linealmente a intervalos iguales, una forma de establecer las vecindades de cada una de ellas, es considerar las células vecinas a una dada como todas aquellas que se encuentran a una distancia menor o igual a una cantidad *r*, llamada radio de vecindad, fijada de antemano. Por ejemplo, las células vecinas a la que ocupa la posición i, en un esquema de vecindad de radio $r = 1$, son las que ocupan las posiciones $i - 1$, i e $i + 1$.

En el caso de dos dimensiones, si las células se colocan sobre los nodos de una malla rectangular, la vecindad de cada una suele estar formada por las cuatro células más próximas (Norte, Sur, Este y Oeste), las ocho más próximas (Norte, Noreste, Este, Sureste, Sur, Suroeste, Oeste, Noroeste) u otras vecindades más amplias.

Conjunto de estados. En cada instante, cada elemento deberá encontrarse en un cierto estado. El caso más sencillo corresponde a los elementos binarios, los cuales se pueden encontrar en sólo uno de dos estados posibles, *0* y *1*, por ejemplo. Pero también el estado puede venir representado por un vector de componentes reales o por cualquier otro conjunto.

Regla de transición local. La regla de transición define la dinámica del sistema. Dado un elemento y un instante determinado, la regla devuelve el siguiente estado del elemento. Para ello necesita como argumentos los estados en el instante anterior tanto del elemento considerado como de aquellos que conforman su vecindad. Las reglas de transición pueden ser deterministas o probabilistas, además, no todos los elementos necesitan obedecer a la misma regla.

3.3. MODELO "TWO TERMINAL".

En esta sección se presenta el estudio del problema de continuidad (también llamado "Two Terminal") desde el nodo fuente *S* [3] al nodo de destino *D* [4]. Se considera una red compuesta por *m* nodos, cuya función es propagar el ataque desde un nodo fuente *S* a un nodo de destino *D*. Para determinar si existe conectividad entre el nodo origen y el nodo destino, se requiere conocer si existe al menos un camino entre *S* y *D*. Esta evaluación se puede realizar a través del algoritmo de búsqueda profunda[5] o a través del siguiente procedimiento basado en autómatas celulares.

3.3.1. Problema de Evaluación de la Continuidad, S – D [ROC].

Dentro de un esquema de cálculo basado en Autómatas Celulares, cada nodo *i* de la red es considerado como una célula, cuya vecindad N_i está conformada por aquellos nodos o celdas que están conectados a través de enlaces. El estado de la variable S_i de la célula *i* es binario, y toma el valor de 1 cuando el nodo *i* está activado (activo) y de 0 cuando no está activado (pasivo).

[3] S – Source
[4] D – Destination
[5] Depth First: es un algoritmo que permite recorrer todos los nodos de una red o árbol de manera ordenada, pero no uniforme. Su manera de funcionar se basa en ir expandiendo cada uno de los nodos que va localizando, de manera recursiva, recorriendo todos los nodos de un camino concreto. Cuando ya no quedan más nodos por visitar en este camino, regresa hacia atrás (backtracking), de tal manera que comienza el mismo proceso con cada uno de los hermanos del nodo ya procesado.

La regla de la transición que gobierna la evolución de la célula *i* en cada instante *t*, consiste en la aplicación del operador lógico OR ($\vee$) a los estados de los nodos en su vecindad:

$$s_i(t+1) = s_p(t) \vee s_q(t) \vee ... \vee s_r(t), \quad p,q,...,r \in N_i \qquad (3.1)$$

Según esta regla, una célula se activa si hay por lo menos una célula activa en su vecindad.

Inicialmente, el nodo fuente *S* es la única célula activa. El uso sucesivo de la regla de transición en cada nodo de la red, genera las trayectorias de la transmisión a través de la red. El cálculo termina cuando se activa el nodo destino o el proceso se estanca: en este caso, no existe conexión entre *S* y *D*. Se considera una red *m* – nodos.

El algoritmo básico procede de la siguiente manera:

1. t = 0,

2. Fije todos los valores del estado de las células a 0 (pasivo),

3. Fije $s_s(0) = 1$ (Fuentes activadas),

4. t = t + 1,

5. Actualice todos los estados de las células por medio de la regla (3.1),

6. Si $s_D(t) = 1$, parar (Destino activado), de lo contrario,

7. Si t < *m* – 1, vaya a 4, de lo contrario,

8. $s_D(m-1) = 0$ (Destino no activado): no hay conexión desde *S* a *D*.

La figura 3.1 muestra un ejemplo de aplicación. Se desea determinar si existe un camino entre el nodo *S* y el nodo terminal *t*.

Inicialmente se activa el nodo *S*. En la iteración 1 *(t*=1*)* se activan los nodos 1, 2, 3 y 4. La figura 3.1.b muestra el estado de la red en *t* = 1. Los nodos que se muestran

punteados corresponden a nodos activados. En t = 2, se activan los nodos 5, 7, 8 y 9, ya que alguno de los nodos de sus respectivas vecindades han sido activados. La figura 3.1.c muestra el estado de la red en t = 2. En la próxima iteración (t=3), el nodo 5 activa al nodo 6 y el nodo 7 activa el nodo final t (ver figura 3.1.d). Como el nodo terminal t ha sido activado, existe conectividad entre S y t.

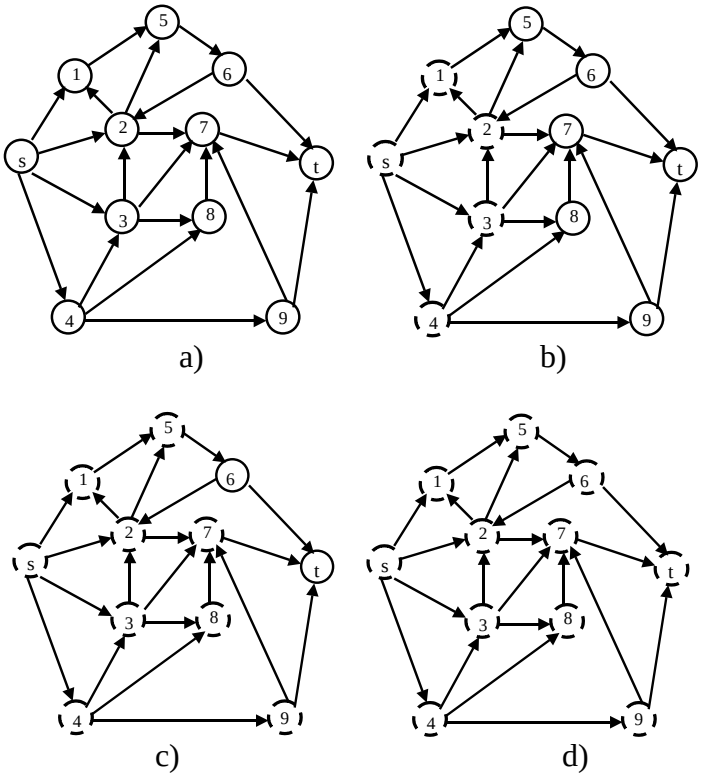


Figura 3.1: Aplicación de Autómata Celular: a) t=0; b) t=1; c) t=2; d) t=3 [YOO].

3.3.2 Propagación del Problema: Evaluación del tiempo en el que el ataque alcanza un nodo de destino i ($TTRD_i$).

Este problema es similar al 3.3.1., con la diferencia que la activación del nodo actual es demorada por el tiempo requerido para propagar el "ataque", desde un nodo al

otro. A este tiempo se le llamará "tiempo de demora entre el nodo *i* y el nodo *j*" (TD_{ij}). Para este modelo se supone que existe conectividad entre el nodo fuente y el nodo destino.

Según la regla 3.1, una célula se activa, desde el punto de vista de la conectividad, si por lo menos hay una célula activa en su vecindad. Cuando se toma en cuenta el proceso de propagación del ataque, la activación de la célula depende también del tiempo requerido para propagar el "ataque": El tiempo de llegada del "ataque propagado" es determinado como la suma del tiempo actual más la demora. Si varios nodos pueden propagar el "ataque" a un nodo dado, el tiempo de llegada del "ataque" a tal nodo es determinado por el mínimo de los tiempos de la propagación de todos los nodos conectados en su vecindad.

Supongamos que el enlace *ji* desde el nodo *j* hasta el nodo *i* puede encontrarse en dos estados posibles: activo ($w_{ji}(t)=1$) o pasivo ($w_{ji}(t)=0$). La variable $w_{ji}(t)$ define el estado operacional del enlace *ji* en cada tiempo *t*. Inicialmente se tiene que $w_{ji}(t)=0$. Tan pronto como el nodo *j* es alcanzado por el ataque, el estado del enlace *ji*, $w_{ji}(t)$, cambiará de 0 a 1, en $t = t + TD_{ji}$.

La regla de transición que gobierna la evolución de la celda *i* es la siguiente:

$$s_i(t) = [w_{pi}(t) \vee w_{qi}(t) \vee ... \vee w_{ri}(t)] \quad p,q,...,r \in N_i \tag{3.2}$$

El algoritmo básico procede de la siguiente manera:

1. t = 0
2. Fije todos los estado de las células y $w_{ji}(t)$ en 0

3. Fije $s_s(0)=1$ y $w_{si}(t+\mathrm{TD_{sj}})=1$ (Nodo fuente s activado y enlaces que salen desde s activados en t = t + TD_{sj})
4. Actualice todos los estados de las células por medio de la regla 3.2 y actualice todos los enlaces que salen desde cada celda
5. t = t + 1
6. Si $s_D(m-1)=0$, parar (destino activado), de lo contrario vaya a 4.

Puesto que por lo menos existe una trayectoria *S* - *D* en la red, el cálculo termina cuando se activa el nodo terminal. Como se mencionó anteriormente, el tiempo para la activación del nodo de destino se puede calcular usando el algoritmo de Dijkstra, descrito en la sección 2.3. Sin embargo el uso del Autómata Celular proporciona además la secuencia de activación de los nodos. Esta secuencia es necesaria si se quiere evaluar el efecto de la propagación del ataque en función del tiempo.

Para ilustrar este procedimiento, se considerará la red de la figura 2.2, de la sección 2.3.1.

La aplicación del algoritmo de Dijkstra mostró que el tiempo mínimo para llegar al nodo *D*=6 es de 6 unidades (ver tabla II.3). Utilizando Autómata Celular se observa:

Dado un "ataque" en t=0 en el nodo fuente *S*=1, el problema consiste en determinar el tiempo de llegada del peligro al nodo de destino *D*=6. La secuencia de eventos a lo largo de la red es:

t = 0: Se activa el nodo 1 y el "ataque" comienza a propagarse hacia los nodos 2 y 3. El tiempo de llegada al nodo 2 es 0 + 2 = 2 y 0 + 3 = 3 al nodo 3. Esto significa que los nodos 2 y 3 serán activados en t = 2 y t = 3, respectivamente ($w_{12}(2)=1$ y $w_{13}(3)=1$).

t = 1: No se activa ninguno de los nodos durante este tiempo y no alcanza la propagación del ataque a los otros nodos.

t = 2: El ataque alcanza al nodo 2 que entonces se activa: $s_2(2) = [w_{12}(2) \vee w_{32}(2)] = 1)$. El ataque comienza a propagarse del nodo 2 al nodo 4, que será alcanzado posiblemente en 2 + 2 = 4 ($w_{24}(4) = 1$).

t = 3: El ataque alcanza al nodo 3, éste se activa. El ataque comienza a propagarse desde el nodo 3 hacia los nodos conectados 2, 4 y 5 con posibles tiempos de llegada en 3 +1= 4, 3 + 2 = 5 y 3 + 2 =5, respectivamente. Sin embargo, el nodo 2 ya está activado y el nodo 4 será posiblemente activado más temprano, en t=4, a través de la trayectoria 1- 2 - 4.

t = 4: El ataque alcanza al nodo 4 desde el nodo 2. El ataque comienza a propagarse desde el nodo 4 hacia los nodos 5 y 6 con posibles tiempos de llegada en 4 + 2 = 6 y 4 + 3 = 7, respectivamente.

t = 5: El ataque alcanza al nodo 5 desde el nodo 3. El ataque comienza a propagarse desde el nodo 5 hacia el nodo 6 con un posible tiempo de llegada en 5 +1 = 6.

t = 6: El ataque alcanza al nodo de destino 6 desde el nodo 5. El procedimiento finaliza puesto que se ha alcanzado el nodo de destino.

La figura 3.2 muestra la evolución del Autómata Celular que corresponde a la propagación del ataque a través de la red. El eje de *x* contiene los índices de los nodos y a lo largo del eje *y*, el tiempo de evolución del Autómata Celular. Los puntos representan las células activas para cada iteración. Así por ejemplo en *t*=0, sólo el nodo 1 está activado. En *t*=2, sólo el nodo 1 continúa activado. En *t*=2, existen dos nodos activados: el número 1 y el número 2.

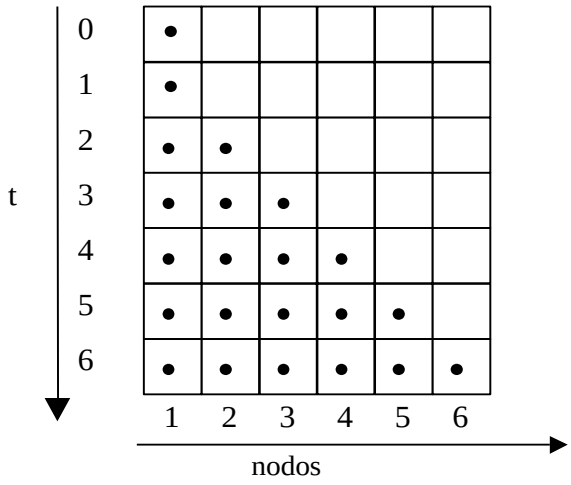


Figura 3.2: Evolución del Autómata Celular para la red de la Figura 2.2.

El uso del modelo basado en Autómata Celular permite evaluar el efecto temporal de las activaciones en los distintos nodos. Por ejemplo, suponemos que el número de personas afectadas por el ataque en varios nodos está dado en la tabla III.1. Entonces, el número de la población afectada en función del tiempo está representado en la tabla III.2.

Tabla III.1: Número estimado de personas afectadas por el ataque en cada nodo.

Nodo	Personas afectadas
1	10
2	20
3	30
4	40
5	50
6	60

Tabla III.2: Evolución del tiempo del número de personas afectadas en la red de la figura 2.2.

Tiempo	Personas afectadas
1	10
2	10 + 20 = 30
3	30 + 30 = 60
4	60 + 40 = 100
5	100 + 50 = 150
6	150 + 60 = 210

En general, el número de personas, en un nodo dado, afectadas por el "ataque" puede ser representado como una variable aleatoria. En éste trabajo se supone que la distribución de las personas afectadas en cada nodo *i* puede ser modelada a través de una distribución uniforme entera, *U[Min(i), Max(i)]*, donde *Min(i)* y *Max(i)* representan los valores inferiores y superiores de esta distribución.

3.4. MODELO "ALL TERMINAL".

El modelo descrito en la sección anterior presenta una limitación ya que es posible que cuando el "ataque" alcanza al nodo de destino, haya nodos que aún no han sido activados.

Por ejemplo, consideremos la red de la figura 2.2, pero ahora con un tiempo de demora igual a 10 unidades para alcanzar el nodo 4 (Ver figura 3.3). La figura 3.4 muestra la evolución del Autómata Celular correspondiente a la propagación del ataque desde el nodo 1 a través de la red. Usando la formulación del problema a) (mediante el

algoritmo de Dijkstra o mediante AC), se obtiene un $TTRD_6$ de 6 unidades. Está claro que el nodo 4 todavía no está activado cuando se alcanza el nodo de destino 6.

El problema a) se puede ampliar para considerar la evaluación del tiempo para alcanzar cada nodo de la red. Este es el problema b) de la sección 3.2 y es similar al problema "All Terminal" considerado en el análisis de la confiabilidad [ZIO].

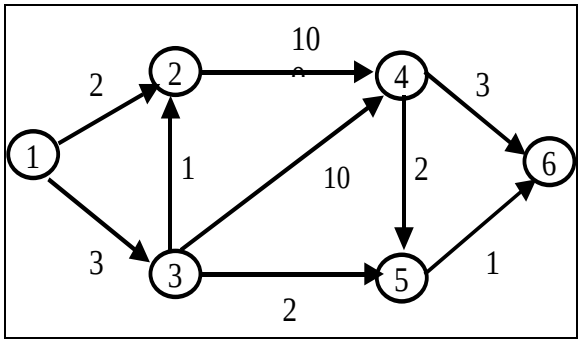


Figura 3.3: Red con tiempos de demora

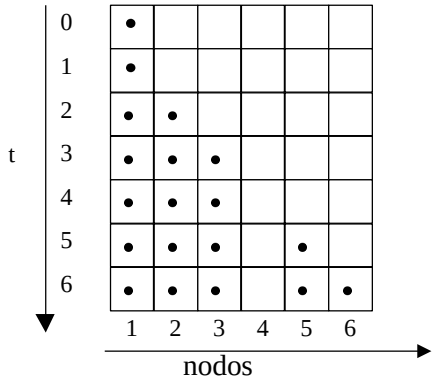


Figura 3.4: Evolución del Autómata Celular para la red de la figura 3.3, usando la formulación del problema a): ataque en $t = 0$ en el nodo 1.

Para realizar la evaluación del Autómata Celular, se introduce un nodo adicional que solamente se activa cuando se activan todos los nodos. Se supone que la red es operativa, es decir, existe por lo menos un árbol de expansión. Usando esta nueva formulación, el nodo 4 se activa en el tiempo 12, según lo mostrado en la figura 3.5. Por tanto, el tiempo para activar todos los nodos es de 12 unidades.

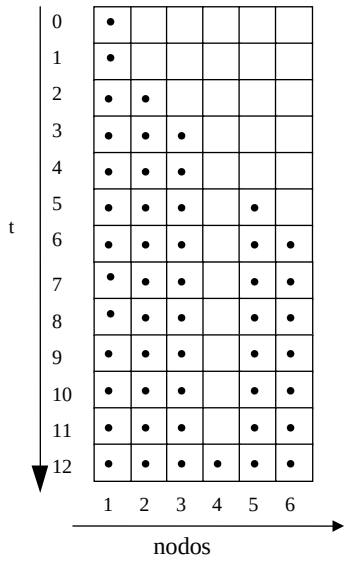


Figura 3.5: Evolución del Autómata Celular para la red de la figura 3.3, usando la formulación del problema b)

La figura 3.6 muestra el árbol de expansión de la figura 3.5. El tiempo mínimo de propagación del ataque es de 12 unidades. Esto se aprecia con las líneas entre cortadas.

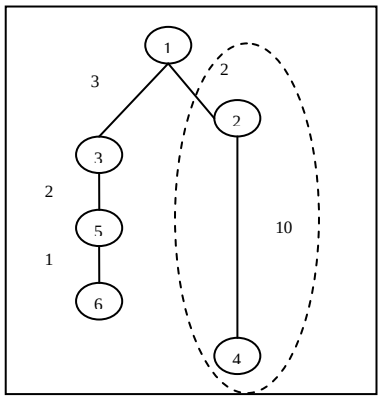


Figura 3.6: Árbol de Expansión para la red de la figura 3.3, usando la formulación del problema b).

En el siguiente capítulo se presentan algunas experimentaciones con los modelos presentados.

CAPÍTULO IV

APLICACIONES

4.1. INTRODUCCIÓN.

En este capítulo se modelan aspectos estocásticos a través de la Simulación Monte Carlo, tales como: el tiempo de propagación del "ataque" entre los nodos de la red así como el número promedio de personas afectadas. Aunado a esto, se usan los modelos de confiabilidad para redes, como son "Two Terminal" y "All Terminal", para evaluar el tiempo cuando el "ataque" alcanza un nodo de destino ***i*** y, para evaluar el tiempo cuando el "ataque" alcanza todos los nodos de la red.

4.2. MODELO TWO TERMINAL.

4.2.1. Evaluación del tiempo cuando el ataque alcanza un nodo de destino.

Para la realización de este análisis, se considera la red representada en la figura 4.1. Esta figura muestra una red dirigida de 11 nodos y 21 enlaces [YOO]. Los nodos 10 y 11 son los nodos Origen *S* y Destino *D*, respectivamente. El tiempo de demora de cada enlace es seleccionado aleatoriamente a través de una distribución uniforme entera entre [0,10]. La evolución de la propagación del "ataque" es repetida 1000 veces a través del programa "Riesgo6corr"[1].

El número de personas afectadas en un nodo dado, es representado como una variable aleatoria entera distribuida uniformemente, *U*[*Min(i)*, *Max(i)*]. En la tabla IV.1., se describe el número de personas afectadas de la red de la figura 4.1.

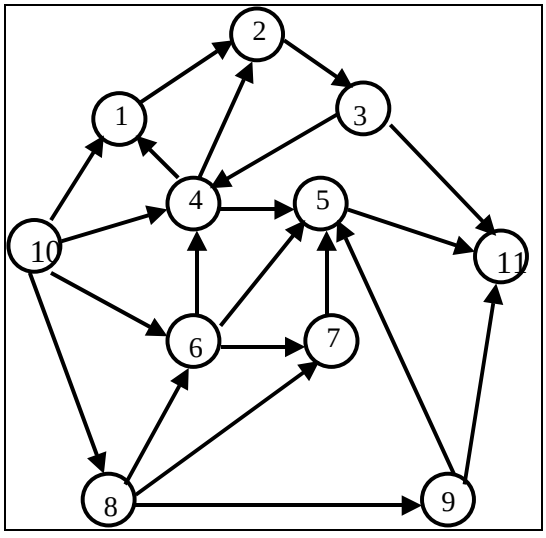


Figura 4.1: Red dirigida de 11 nodos y 21 enlaces.

[1] Programa para calcular la propagación del ataque desde un nodo *i* a un nodo *j*.

Tabla IV.1: Número de personas afectadas de la red de la figura 4.2.

Nodo	Min	Max
1	10	20
2	15	40
3	5	20
4	20	30
5	40	60
6	10	30
7	10	20
8	15	40
9	5	20
10	20	30
11	40	60

La figura 4.2 muestra la distribución del tiempo de activación de la red de la figura 4.1, cuando el "ataque" alcanza el nodo de destino 11. ($TTRD_{11}$). El tiempo promedio para alcanzar el nodo 11 es de 10.869 unidades.

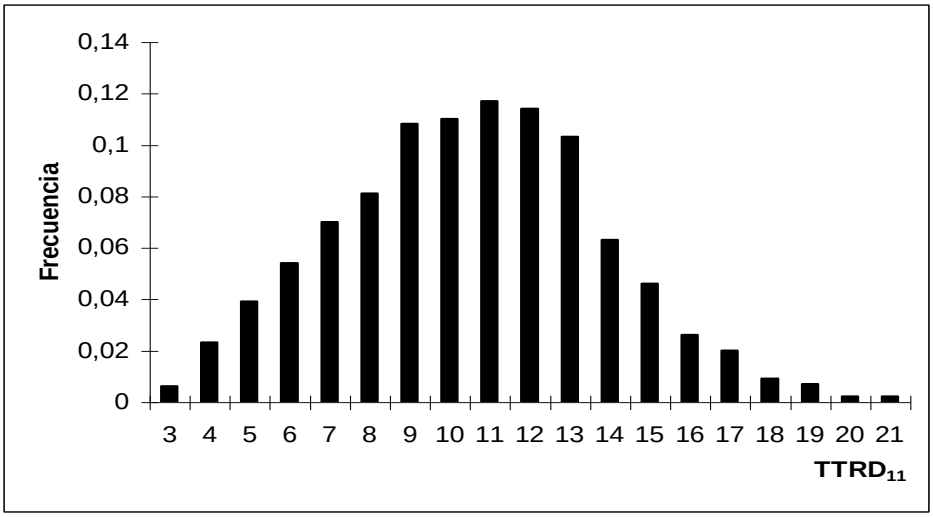


Figura 4.2: Distribución de los tiempos de activación del nodo 11.

El número de personas afectadas por el ataque a medida que los nodos se van activando, se muestra en la figura 4.3., donde el promedio de personas afectadas es de 432,36.

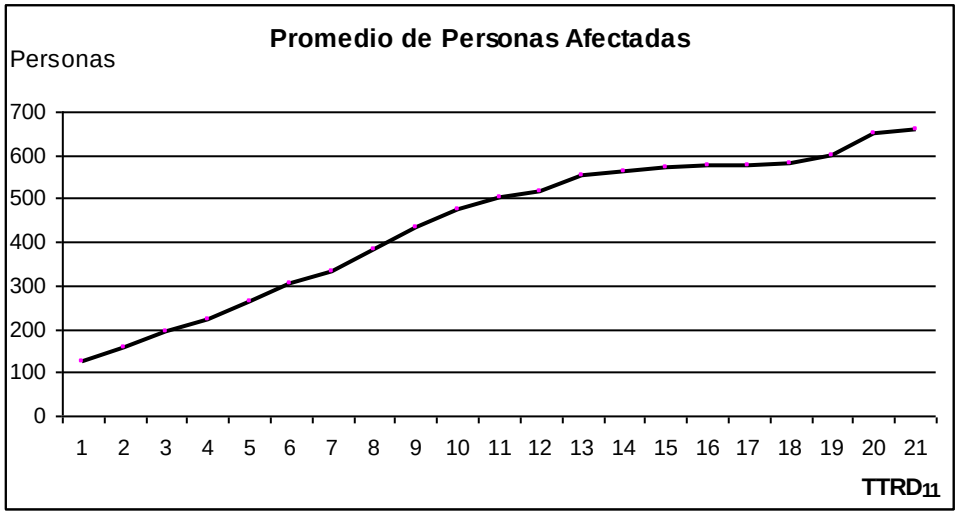


Figura 4.3: Promedio de personas afectadas de la red de la figura 4.1

4.2.2. Acciones a tomar.

El modelo "Two Terminal" puede usarse para evaluar posibles estrategias para contrarrestar el efecto de ataques. Por ejemplo, es posible evaluar si la eliminación de un enlace puede retardar la llegada del efecto de un ataque.

En la tabla IV.2 muestra los tiempos promedio de activación y promedio de personas afectadas por la red 4.1 al eliminar sistemáticamente cada enlace. (La eliminación de un enlace *ij*, se modela colocando un $TD_{ij} = \infty$, esto es un tiempo de propagación muy grande).

Al eliminar el enlace 9 – 5, se obtiene que el tiempo promedio de activación del nodo 11 más alto, es de 16.92 unidades. Ahora bien, si eliminamos el enlace 4 – 2, se obtiene el promedio de personas afectadas más alto, de 429.04. Por tanto, la decisión a tomar deberá considerar ambos efectos.

Ahora bien, la eliminación del enlace 6 – 7, hace que la red sea más vulnerable, ya que el tiempo de propagación del ataque se realiza en un tiempo de 10.39 unidades. (Menor tiempo).

Tabla IV.2: Tiempo promedio de alcance del ataque y promedio de personas afectadas de la red de la figura 4.1.

Enlace Eliminado	Tiempo Promedio	Promedio Personas Afectadas
1-2	10.89	399.74
2-3	11.09	417.07
3-4	11.02	405.85
3-11	11.32	420.81
4-1	11.11	396.15
4-2	**10.65**	**424.09**
4-5	10.78	395.98
5-11	13.82	419.36
6-4	10.71	415.31
6-5	11.32	416.83
6-7	10.39	410.19
7-5	11.15	406.32
8-6	10.94	409.09
8-7	10.59	405.82
8-9	11.89	395.94
9-5	**16.92**	**410.70**
9-11	12.04	409.81
10-1	10.86	405.46
10-4	11.80	413.20
10-6	11.90	396.14
10-8	12.48	314.48

4.3. MODELO "ALL TERMINAL".

Para evaluar este modelo, se utilizaron los programas: "GeneraST[2]" y "Exbomio1[3]" desarrollados por el Departamento de Investigación de Operaciones, Facultad de Ingeniería de la Universidad Central de Venezuela. Estos programas calculan el tiempo de propagación del ataque y el promedio de personas afectadas.

El ejemplo seleccionado es una central telefónica [MAN], como se muestra en la figura 4.4, definida como una red no dirigida compuesta por 52 nodos y 73 enlaces. Los enlaces que poseen cada nodo, están descritos en la tabla No. IV.4. El tiempo de demora en cada enlace es seleccionado a través de una distribución uniforme entera entre [0,10]. La evolución de la propagación es repetida 1000 veces. El número de personas afectadas en un nodo dado, es representado como una variable aleatoria entera distribuida uniformemente, $U[Min(i), Max(i)]$, donde $Min(i)$ y $Max(i)$ están definidas por como se muestra en la tabla IV.3.

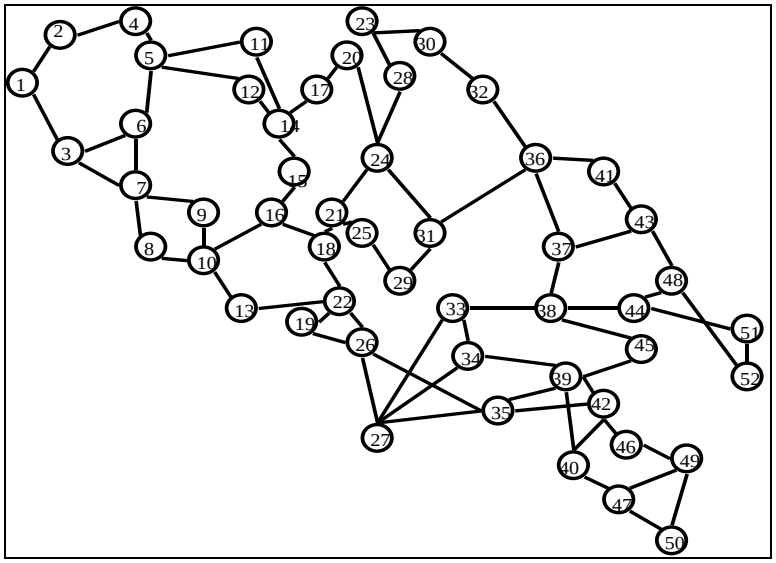


Figura 4.4: Red Telefónica

[2] Programa para calcular la propagación del ataque sin inmunización.
[3] Programa para calcular la propagación del ataque con inmunización de nodos.

Tabla IV.3 – Números de nodos y cantidad de enlaces

Nodo No	enlaces	Nodo No	enlaces	Nodo No	enlaces	Nodo No	enlaces
1	2	**14**	4	**27**	4	**40**	3
2	2	**15**	2	**28**	2	**41**	2
3	3	**16**	3	**29**	2	**42**	5
4	2	**17**	2	**30**	2	**43**	3
5	4	**18**	3	**31**	3	**44**	3
6	3	**19**	2	**32**	2	**45**	2
7	4	**20**	2	**33**	3	**46**	2
8	2	**21**	3	**34**	3	**47**	3
9	2	**22**	4	**35**	4	**48**	3
10	4	**23**	2	**36**	4	**49**	3
11	2	**24**	4	**37**	3	**50**	2
12	2	**25**	2	**38**	4	**51**	2
13	2	**26**	4	**39**	4	**52**	2

Tabla IV.4 Números de personas afectadas para red de la figura 4.1.

Nodo	Min	Max	Nodo	Min	Max	Nodo	Min	Max	Nodo	Min	Max
1	17	32	**14**	17	35	**27**	15	39	**40**	11	38
2	16	36	**15**	12	37	**28**	10	40	**41**	13	32
3	11	33	**16**	20	40	**29**	19	35	**42**	14	34
4	12	38	**17**	12	31	**30**	17	37	**43**	20	39
5	19	38	**18**	15	31	**31**	14	37	**44**	18	32
6	19	33	**19**	18	34	**32**	17	31	**45**	15	34
7	13	30	**20**	13	30	**33**	12	38	**46**	20	33
8	14	31	**21**	15	33	**34**	17	40	**47**	19	36
9	19	40	**22**	10	31	**35**	18	39	**48**	16	38
10	15	38	**23**	18	39	**36**	11	33	**49**	13	31
11	13	39	**24**	16	32	**37**	11	37	**50**	16	37
12	13	39	**25**	14	40	**38**	13	35	**51**	18	36
13	14	34	**26**	15	36	**39**	16	34	**52**	13	35

4.3.1 Evaluación del tiempo en el que el "ataque", alcanza todos los nodos de la red. (TTRAD)[4].

Para la realización de las simulaciones, se consideró que un nodo es atacado a la vez y en ese momento el ataque se propaga por toda la red. Esta operación se repite 52 veces, (una vez para cada nodo).

Se analizarán el tiempo mínimo de activación, el tiempo máximo de activación y el tiempo promedio de activación. (El tiempo de activación se define como el tiempo en que el ataque se propaga a través de toda la red)

1. Tiempo Mínimo de activación.

La figura 4.5 representa el tiempo mínimo de activación para diversos nodos atacados. Los resultados obtenidos indican que el ataque en el nodo 51 produce un tiempo mínimo de activación de 32 unidades, mientras que el ataque en el nodo 27 resulta una propagación de 19 unidades. Esto indica que el ataque perpetrado en el nodo 27 se propaga más rápido a través de toda la red, siendo este nodo el que convierte a la red en más vulnerable.

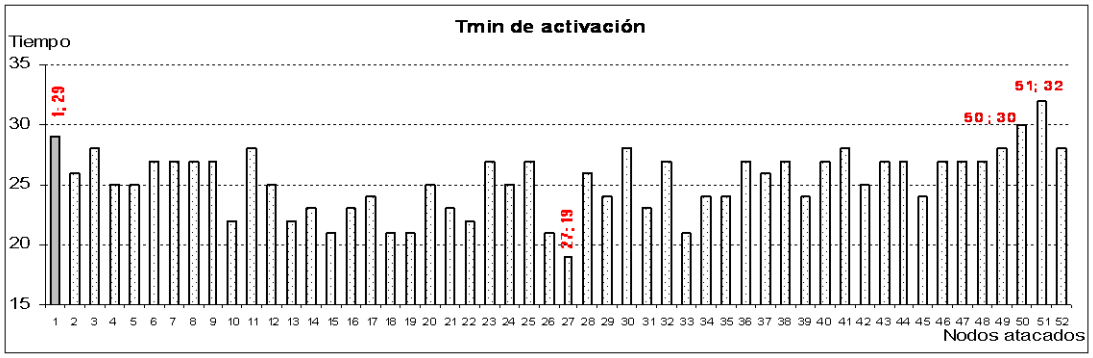


Figura 4.5. Tiempo mínimo de activación para distintos nodos atacados.

[4] TTRAD – Total Time to Reach All Destination.

2. Tiempo Máximo de activación.

La figura 4.6 representa el tiempo máximo de activación para diversos nodos atacados. Los resultados obtenidos indican que el ataque en el nodo 2 produce un tiempo máximo de activación de 94 unidades, mientras que el ataque en el nodo 22 resulta un tiempo de propagación de 50 unidades.

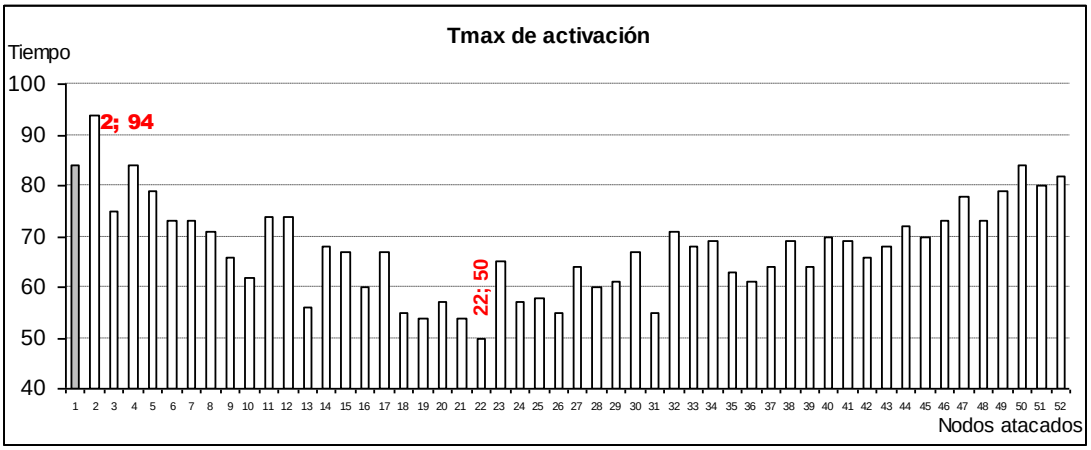


Figura 4.6: Tiempo máximo de activación para distintos nodos atacados.

3. Tiempo Promedio de activación.

La figura 4.7 representa el tiempo promedio de activación para diversos nodos atacados. Los resultados obtenidos indican que el ataque en el nodo 2 produce un tiempo promedio de activación de 57 unidades, mientras que el ataque en el nodo 22 resulta una propagación de 35 unidades. Esto indica que el ataque en el nodo 22 se propaga en promedio más rápido a través de toda la red.

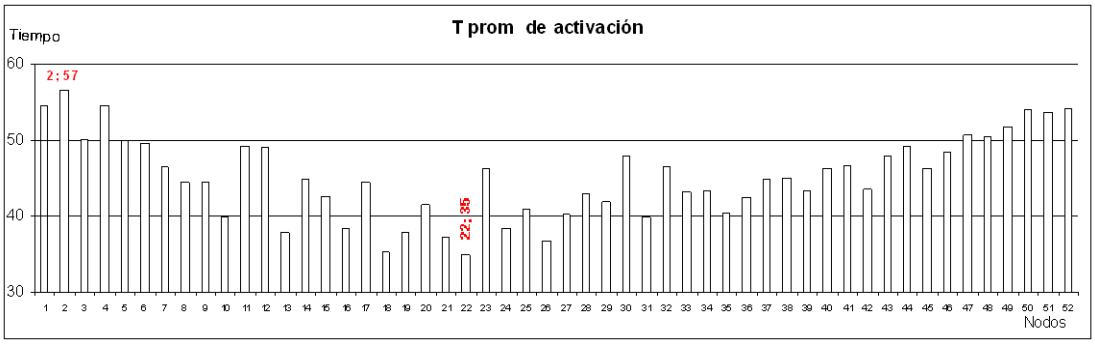


Figura 4.7: Tiempo promedio de activación para distintos nodos atacados.

4. Cantidad de personas afectadas.

La figura 4.8 presenta la cantidad promedio de personas afectadas cuando el ataque es perpetrado en cada nodo de la red. Este resultado muestra que el nodo 38 posee el mayor valor promedio de personas afectadas con un valor de 939 personas, siendo éste el nodo que convierte a la red más vulnerable. Es importante destacar que éste nodo no es reflejado en ninguna de las figuras 4.5, 4.6 y 4.7, lo que indica que la evolución del ataque en la red deberá considerar por ejemplo ambos aspectos. El nodo 23, representa un valor de 797 personas afectadas, siendo éste el valor más bajo.

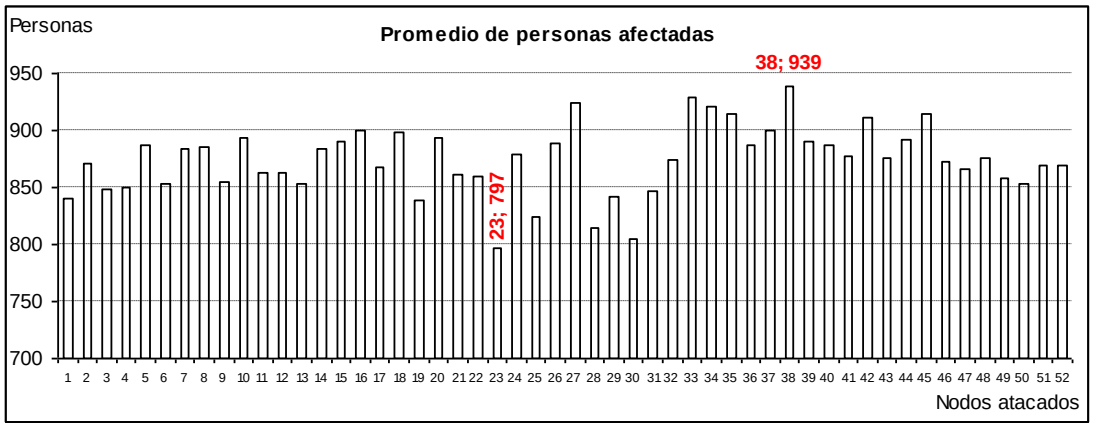


Figura 4.8: Promedio de personas afectadas para distintos nodos atacados.

Para ilustrar el efecto de un ataque en el número de personas afectadas, se escogen cinco nodos cualesquiera: 22, 18, 26, 21 y 13. La figura 4.9 muestra cómo a medida que se difunde el ataque varía el número promedio acumulado de personas afectadas. Se nota claramente que el efecto del ataque en el nodo 22 es que afecta más rápido. En este caso, el ataque a este nodo causa mayor vulnerabilidad a la red.

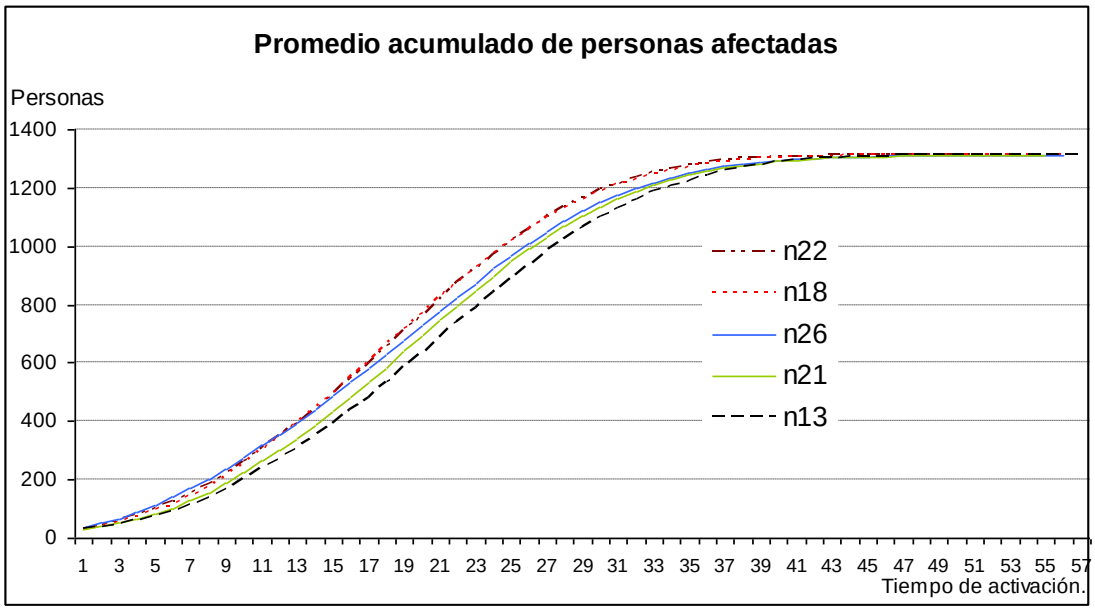


Figura 4.9: Promedio acumulado de personas afectadas en función del tiempo de activación de los nodos.

4.3.2. Evaluación del efecto de inmunización de los nodos.

Para la realización de este análisis, se consideraron los siguientes aspectos:

a) El nodo atacado se mantiene constante y se inmuniza uno a uno el resto de los nodos de la red, obteniéndose así 2704 (52 X 52) corridas.

b) Se utiliza la estrategia de inmunización, el ataque no afecta al nodo que se inmuniza y éste no propaga el ataque.

Para ilustrar los resultados de este estudio, se consideró el nodo 1.

La figura 4.10 muestra la comparación del tiempo promedio de activación cuando el ataque es perpetrado en el nodo 1 de la red 4.4 sin inmunizar y b) Cuando se realiza la inmunización uno a uno al resto de los nodos. Estos resultados indican que el tiempo de activación promedio cuando los nodo uno a uno son inmunizados es mayor que cuando no son inmunizados. El mejor tiempo se obtiene inmunizando los nodos 22, 24 y 26. Note que estos nodos poseen cada uno 4 enlaces, ver tabla IV.3. Es importante resaltar que esta desviación entre estas dos curvas, muestra la vulnerabilidad de la red cuando se inmuniza y no se inmuniza.

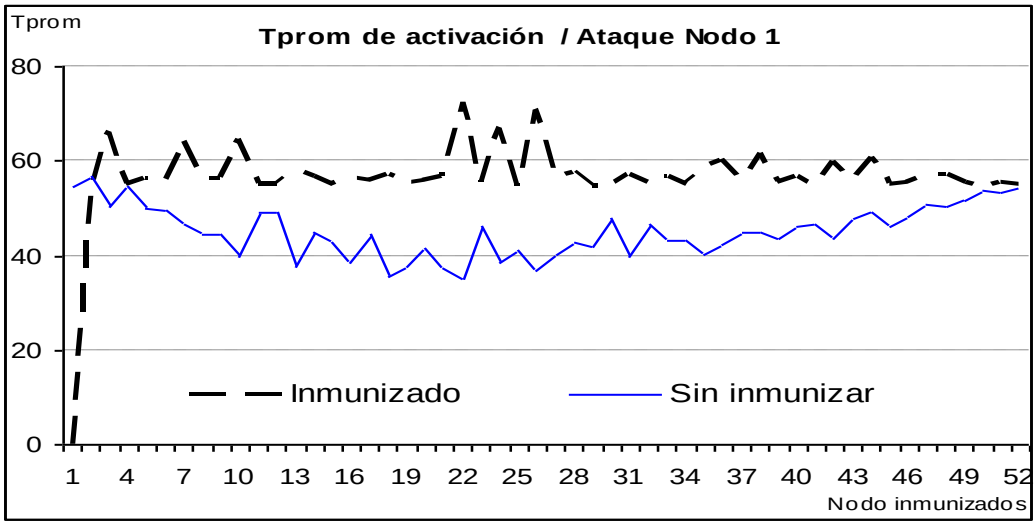


Figura 4.10: Comparación del tiempo promedio de activación a) cuando el ataque es perpetrado en el nodo 1 sin inmunizar y a) inmunizando los nodos.

La figura 4.11, representa el tiempo promedio de activación cuando el ataque es perpetrado en el nodo 1 y el resto de los nodos son inmunizados uno a uno. Los resultados obtenidos indican que cuando se inmuniza el nodo 22, se obtiene un tiempo promedio de activación de 72 unidades, mientras que la inmunización en el nodo 50 resulta en una propagación de 54 unidades, siendo éste el valor más bajo.

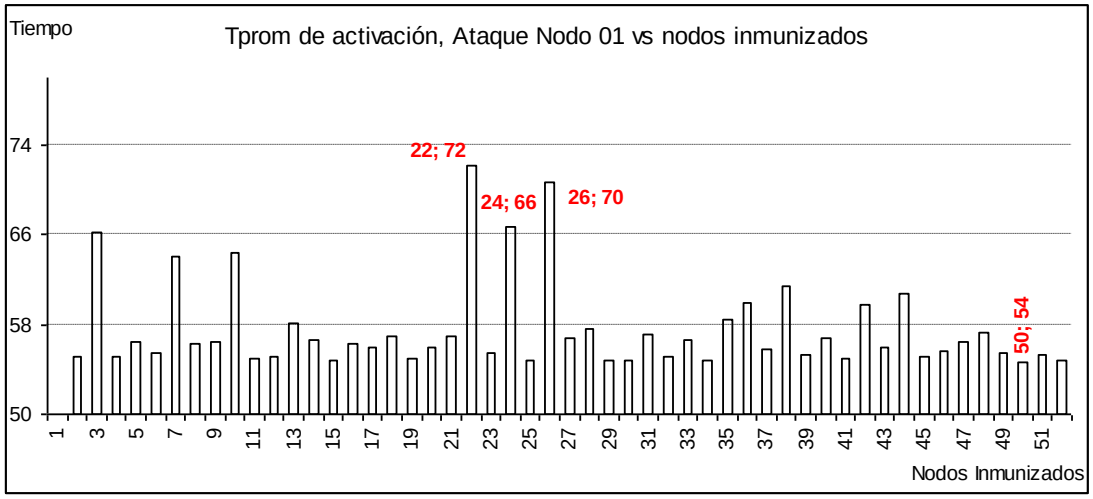


Figura 4.11: Tiempo de activación promedio, ataque nodo 1 vs. nodos inmunizados.

En la figura 4.12 se muestra la comparación del promedio de personas afectadas en función del tiempo de activación, cuando el nodo 24 está inmunizado y el ataque es perpetrado en el nodo 1 y cuando el nodo 24 no está inmunizado. Esta figura muestra que cuando el nodo 24 no está inmunizado produce un número mayor de personas afectadas con relación al nodo inmunizado, al estar esta curva por encima de la curva inmunizada.

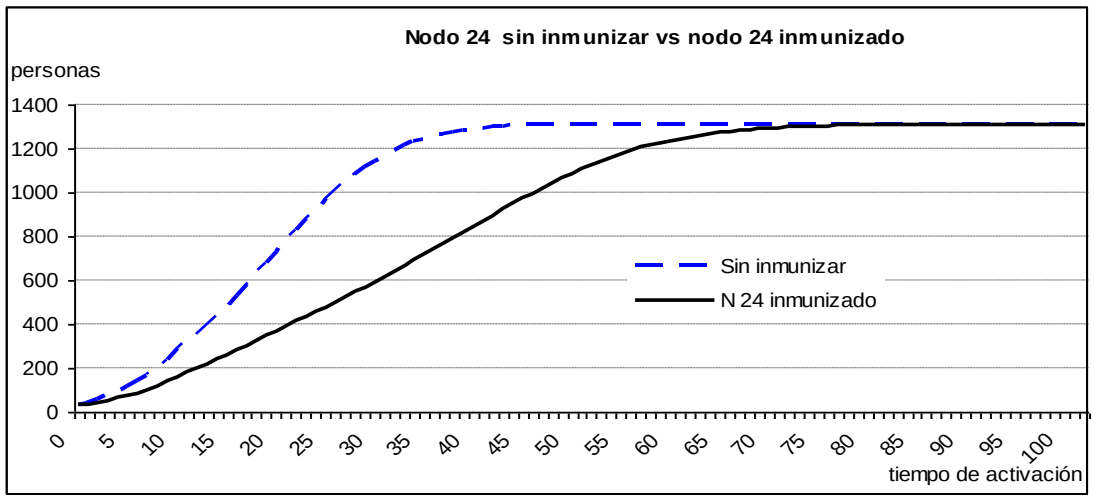


Figura 4.12: Comparación del promedio de personas afectadas para el nodo 24 sin inmunización vs. inmunizado.

La figura 4.13 presenta el promedio de personas afectadas en función de la evolución del tiempo de propagación. En este caso se obtiene que la inmunización del nodo 24 produce mayor valor promedio de personas afectadas, mientras que la inmunización en el nodo 3 representa el menor valor.

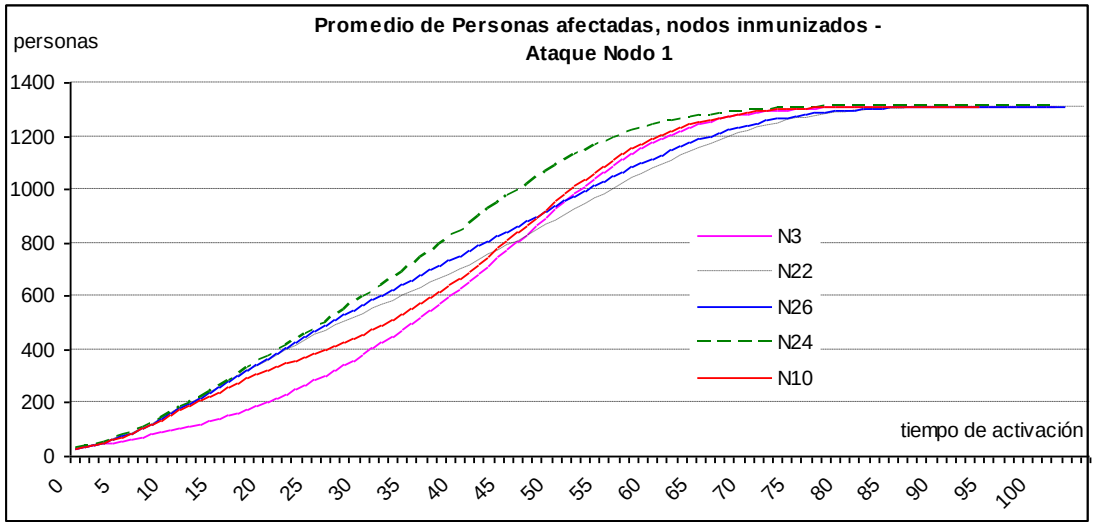


Figura 4.13: Promedio de personas afectadas en función al tiempo de activación de los nodos, ataque nodo 1, restos de nodos inmunizados.

El modelo “All Terminal” permite analizar si existe algún nodo o grupo de nodos que resulte consistentemente como mejor nodo a inmunizar. Para esto, se seleccionan aleatoriamente los nodos: 1, 2, 4, 15, 20, 52, se perpetra el ataque en estos nodos y se inmuniza el resto uno a uno. La tabla IV.5 muestra que para cada nodo “atacado” y dependiendo del criterio usado, presenta el nodo que produce “mejores” resultados. Por ejemplo, si el ataque se realiza en el nodo 4 y el criterio evaluado es el tiempo promedio, el mejor nodo a inmunizar resultó ser el nodo 24. Si sumamos el número que se repiten los nodos inmunizados, se obtiene que el nodo 24 resulta ser consistentemente menor nodo a inmunizar, seguido del nodo 22. (Ver figura 4.14).

Tabla IV.5. Frecuencia de nodos inmunizados con ataques en los nodos 1,2, 4, 15, 20, 50, 52.

Ataque en nodo	Tiempo Promedio		Tiempo Máximo		Promedio de personas afectadas	
	Mejor nodo a inmunizar	T prom	Mejor nodo a inmunizar	T max	Mejor nodo a inmunizar	Personas afectadas
1	22	72	22	105	22	842
2	22	72	**24**	112	**24**	907
4	**24**	68	**24**	105	**24**	898
15	22	58	22	85	**24**	941
20	**24**	69	**24**	102	**24**	854
50	26	72	26	111	22	875
52	38	67	5	100	52	867

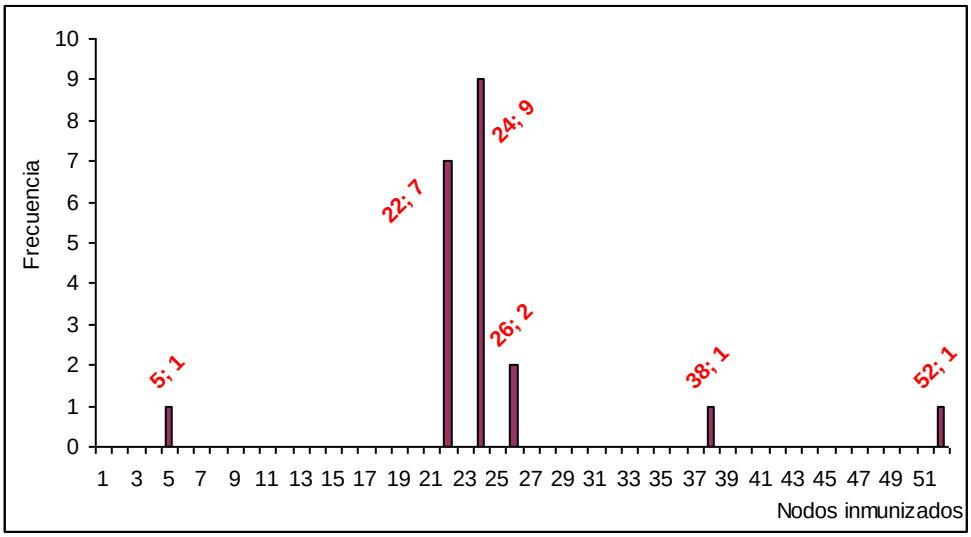


Figura 4.14: Representación gráfica de la frecuencia de nodos inmunizados con ataques en los nodos 1,2, 4, 15, 20, 50, 52.

Para ilustrar el comportamiento del nodo 24 ante diversos ataques y estudiar el promedio de personas afectadas, se tomaron los nodos atacados de la tabla IV.5. La figura 4.15 muestra que cuando el ataque es perpetrado en el nodo 15, el nodo inmunizado 24 posee el mayor valor promedio de personas afectadas mientras que en el ataque en el nodo 20, el nodo inmunizado 24 posee el menor valor.

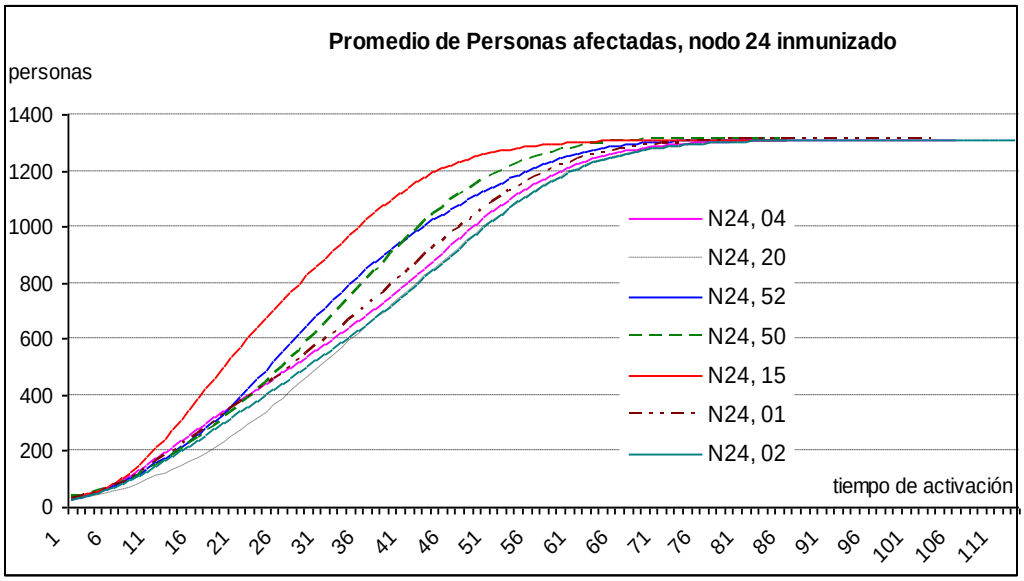


Figura 4.15: Promedio de personas afectadas, nodo 24 inmunizado y ataques en los nodos 01, 02, 04, 15, 20, 50, 52.

Una vez realizado las distintas corridas evaluando el tiempo que tardan los efectos del ataque en alcanzar un nodo específico y evaluando el tiempo que tardan los efectos del ataque en alcanzar todos los nodos, utilizando los criterios de confiabilidad “Two Terminal” y “All Terminal”, se llegan a las conclusiones descritas en el próximo capítulo.

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES.

En este trabajo se presenta el desarrollo de un marco referencial de modelos matemáticos que permiten estudiar la vulnerabilidad de una red, la cual se entiende como la exposición latente a un riesgo, es decir, una mezcla compleja de amenazas bien sea humanas o naturales que sostienen un entorno social, político y económico.

El representar estos entornos específicamente en una red, permite conocer el comportamiento así como evaluar la seguridad de la misma. Esta seguridad se estudió a través de la propuesta de dos modelos para hallar el tiempo mínimo de propagación de un ataque, con la implementación de los algoritmos de Dijkstra y Árbol de Expansión mínima. Estos modelos nacen como una interpretación de dos criterios ampliamente utilizados en la evaluación de la confiabilidad de una red.

Aunado al tiempo de propagación del ataque en la red, se propuso un modelo de evaluación de las consecuencias de un ataque, mediante la determinación del número de personas afectadas a medida que evoluciona el ataque. Este problema se resolvió a través del enfoque de Autómata Celular.

Aspectos probabilísticos asociados al tiempo de propagación y al número de personas afectadas se evaluaron a través de modelos basados en Simulación Monte Carlo.

Los modelos presentados permiten:

- Identificar los enlaces y nodos más importantes de la red, en función del tiempo que tarda un ataque en propagarse por la red.

- Identificar los nodos más importantes de la red, en función del efecto que un ataque puede ocasionar en dichos nodos o en el sistema (por ejemplo, analizando el promedio de personas afectadas).

- Establecer niveles de prioridad e importancia de los nodos en la red, para así manejar la emergencia del ataque identificando por ejemplo los enlaces o nodos que deben aislarse para minimizar las consecuencias.

RECOMENDACIONES.

El Trabajo permite definir un marco de referencia para el estudio de la vulnerabilidad de una red ante un ataque. Por tanto se recomienda extender los modelos aquí propuestos con la incorporación de modelos adicionales que permitan:

a) Experimentar diferentes consecuencias

b) Proponer otros esquemas de protección/inmunización

c) Considerar la factibilidad del diseño óptimo de tales redes

d) Extender los conceptos de medidas de importancia definidos en la evaluación de la confiabilidad de una red, para aplicarlos a la jerarquización de nodos y enlaces, bajo la óptica de ataque.

Es importante tomar en consideración, que las amenazas no disminuirán y las vulnerabilidades no desaparecerán en su totalidad, por lo que los estudios deberán siempre hacerse y estar acordes con la importancia del riesgo. Esto sugiere otra posible línea de investigación que involucre la consideración de aspectos tantos técnicos (por ejemplo: cómo, dónde y cuándo realizar la inmunización) y aspectos monetarios (por ejemplo: costos y beneficios de tales inmunizaciones).

BIBLIOGRAFÍA

[AHO] **Alfred Aho, John Hopcroft, Jeffrey Ullman**, (1988). Estructura de Datos y Algoritmos. Addison Wesley Iberoamericana, S. A. Washington. Cáp. 6 y Cáp. 7 pp. 200-251.

[APO] **George Apostolakis**, (2005). Protecting Infrastructures: The role of risk analysis. Safeguarding National Infrastructures: Integrated approaches to Failure in Complex networks.

http://www.dcs.gla.ac.uk/~johnson/infrastructure/papers/Apostolakis_keynote.pdf

[BIL] **Roy Billinton**, **Roland Allan**, (1992) Reliability Evaluation of Engineering Systems, Second Edition. New York: Plenum Press, Cáp. 13.

[BOD] **Hans L. Bodlaender, Thomas Wolle**, (2004). A Note on the Complexity of Network Reliability Problems. Technical report UU-CS-2004-001.
http://www.cs.uu.nl

[BRA] **L.A. Braunstein, S.V. Buldyrev**, (2005) Threat Networks and Threatened Networks: Basic Principles and Practical Applications. http://polymer.bu.edu/~hes/networks/lellenberg-viewgraphs.pdf

[CAM] **Rahn Campos**, (2002) Algoritmo Evolutivo para el Problema de Árbol de Mínima Expansión.
http://www.alfredorahn.com/docs/GMSP_Paper.pdf

[CHA] **Sarah Chandler, Robert Watt**, (2005) Point of View on UK Counter Terrorism. Hewlett Packard Development Company.

h40059. www4.hp.com/counterterrorism/ 118_2023_Counter_Terrorism.pdf.

[COL] **Colburn Charles**. (1987). The Combinatorics of Network Reliability. Oxford Unirvesity Press. Cáp. 1, pp. 1-7.

[DOR] **S. N. Dorogovtsev, J. F. F. Mendes**, (2004). The Shortest Path to Complex Networks.
http://arxiv.org/abs/cond-mat/0404593

[FON] **Luciano da Fontoura Costa**, (2005), A Generalized Approach to Complex Networks. University of Sao Paulo.
http://arxiv.org/PS_cache/cond-mat/pdf/0408/0408076.pdf

[GAR] **Arcadio Rubio García**, (2004), Determinar la Ruta más Corta Entre Dos Vértices de un Grafo Conexo con Pesos Positivos.
http://petra.euitio.uniovi.es/asignaturas/teo.pro/trabajos/2004/soluciones/Dijkstra.pdf

[GER] **Timothy C. Germain, Kai Kadau, Ira Longini, Catherine Macken**, (2006), Mitigation Strategies for Pandemic Influenza in the United States. Vol 103-15
http://www.pnac.org/cgi/10.1073.

[GON] **Goncharova A**, **Ball M.O., Colbourn C.J., Provan J.S.** (1992), Network Reliability, R. 92-74.
http://book.itep.ru/4/45/network_r.htm

[HER] **Jose Gregorio Hernandez**, (2003). Árboles Generadores Mínimos (MST), Teoría de Grafos 02- 03.
http://www.dma.fi.upm.es/gregorio/grafos/mst03.PDF.

[HILL] **Frederick Hiller**, (1991). Introducción a la Investigación de Operaciones, Mc Graw Hill. Segunda Edición, Cáp. 10, pp. 333 – 391.

[HOL] **Holmgren, Å., Molin, S., Thedéen, T.,** (2002). Vulnerability of Complex Infrastructure, Power Systems and Supporting Digital Communication Systems.

http://www.delft2001.tudelft.nl/paper%20files/paper1089.doc

[JOH] **C.W. Johnson,** (2005). Using Violation and Vulnerability Analysis to Understand the Root-Causes of Complex Security Incidents. University of Glaslow.
http://www.dcs.gla.ac.uk/~johnson.

[MAN] **Manzi E., Labbé M., Latouche G., Maffioli F**. (2001) Fishman´s Sampling Plan Computing Network Reliability. IEEE Trans Reliab, R – 50:41-46.

[MER] **Juan Merelo**, Redes Sociales, (2005). Revista Hispana para el Análisis de Redes Sociales. Universidad de Grenada.
http://revista-redes.rediris.es/webredes/talleres/redes-sociales.pdf

[MOS] **Hebert Moscowitz, Gordon Wright**, (1982). Investigación de Operaciones. Prentice Hall Hispanoamericana, S.A. Cáp. 18, pp. 725-727.

[NIS] National Infrastrucutre Security Coordination Centre, (2006), To Minimize the Risk to the Critical National Infrastructure from Electronic Attack.
http://www.niscc.gov.uk/niscc/aboutCNI-en.html.

[REK] **Reka Albert and Albert-Laszlo Barabási**, (2000) Topology of Evolving Networks: Local Events and Universality. University of Glasgow.
http://arxiv.org/PS_cache/cond-mat/pdf/0408/0408076.pdf

[ROC] **Claudio M. Rocco S, Enrico Zio**, (2004). Solving Advanced Network Reliability Problems by Means of Cellular Automata and Monte Carlo Sampling. Reliability Engineering and System Safety. 89 (2005) 219-226.

[SAN] **John Jairo Sánchez C. , Jorge Hernán Restrepo**, (2004). Aplicación de la Teoría de Grafos y el Algoritmo de Dijkstra para Determinar las Distancias y las Rutas más Cortas en una Ciudad.
http://www.utp.edu.co/php/revistas/ScientiaEtTechnica/docsFTP/111527121-126.pdf

[SEA] **Sean A. Patterson and George E. Apostolakis**, (2005) Identification of Critical Locations across Multiple Infrastructures for Terrorist Actions. http://www.dcs.gla.ac.uk/~johnson/infrastructure/papers/Patterson_GEA.pdf.

[SEC] **Securing Critical Infrastructures**, The National Strategy for the Physical Protection of Critical Infrastructure. (2005).

http://www.whitehouse.gov/pcipb/physical/securing_critical_infrastructures.pdf

[TAJ] **Hamdy Taha**, (1995). Investigación de Operaciones, Alfaomega Grupo Editor, S.A. de C.V. Cáp. 8, pp. 315 – 348.

[WIK] **Wikipedia**, (2006).
http://es.wikipedia.org/wiki

[YOO] **Yoo, Y B, Deo, N.** ,(1998) A Comparison Algorithm for Terminal – Pair Reliability IEEE Trans Reliab, R-37.

[ZIO] **Zio. E, Rocco C.**, (2005). Security Assessment in Complex Networks Exposed to Terrorist Hazard: A Methodological approach based on Cellular Automata and Monte Carlo Simulation, Complex Network and Infrastructure Protection CNIP 2006, Roma, Italia.