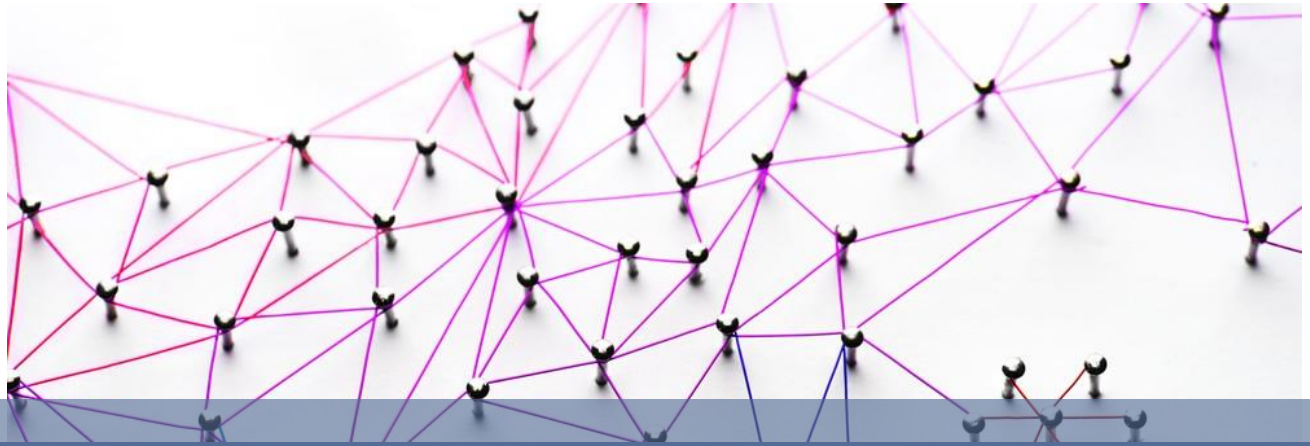
Análisis de un modelo de redes peer-to-peer bajo un ataque cibernético utilizando cadenas de Markov

Natalia Sánchez
Asesores: Dra. Gina Gallegos García
Dr. Mario Rivero Ángeles

Planteamiento del problema



Las redes P2P son ideales para la difusión a una gran cantidad de computadoras. Por medio de este trabajo se investiga el alcance que podría tener este tipo de archivos corruptos a través de una red P2P, así como la importancia de los factores involucrados en el funcionamiento de la red. Para nuestro caso de estudio desarrollamos la simulación de un modelo que emula de manera sencilla el comportamiento de un ataque simple a una red de pares a pares, por lo que se escogió las cadenas de Markov como herramienta para modelar este tipo de redes y su comportamiento bajo un ciberataque general.

Justificación

Estas redes representan actualmente un porcentaje considerable de todo el ancho de banda mundial. Sin embargo, representa una multitud de vulnerabilidades y amenazas a la seguridad. Una consecuencia directa de el no contar con servidores centralizados es que no hay ningún mecanismo para controlar qué contenido se comparte, esto hace que las redes P2P sean óptimas para la propagación de malware en general. Para ello se busca realizar un mecanismo de análisis que ayude a controlar el tráfico de las redes, analizando la cantidad de nodos infecciosos que pueden causarle daño a la red.

Hipótesis

Se pretende presentar un modelo simplificado de una red P2P de manera que se compruebe su correcto funcionamiento para el enlace archivos en continua transmisión, haciendo uso del esquema de cadenas de Markov, además de comprender algunos aspectos del comportamiento de dicho esquema. Buscando conocer cuales son los factores más determinantes para el comportamiento observado.

Objetivo General

Desarrollar un modelo simplificado de una red P2P para poder verificar su rendimiento bajo ese primer esquema simple y entender su comportamiento bajo las condiciones de un ciber-ataque, pudiendo robustecer el modelo tras la identificación de sus debilidades en las simulación de un ataque dentro o hacia la red.

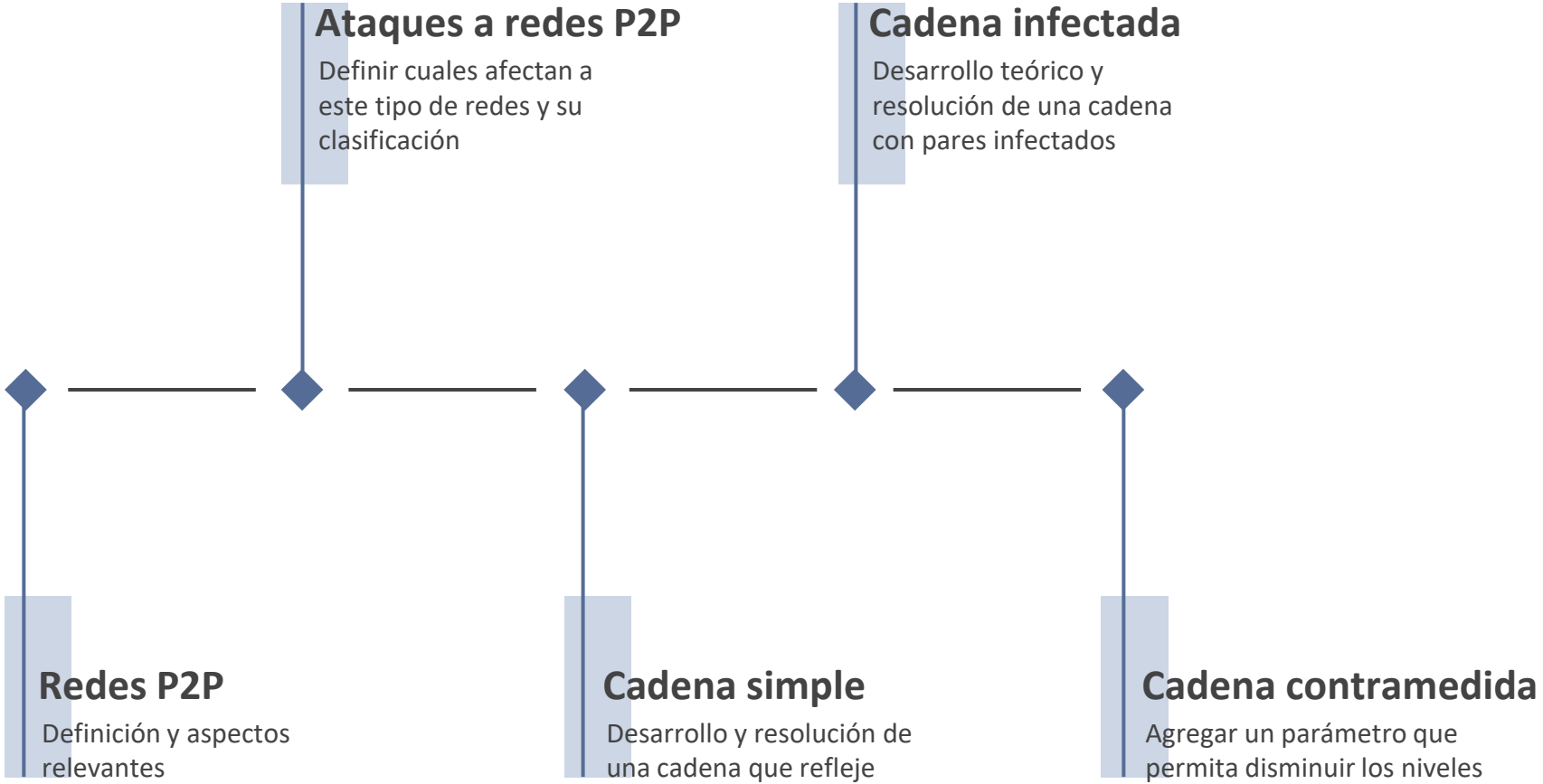
Objetivos Particulares

Analizar el modelo generado utilizando las cadenas de Markov relacionadas con ciber-ataques en redes P2P.

Obtener medidas de desempeño de la red P2P bajo un ciber-ataque

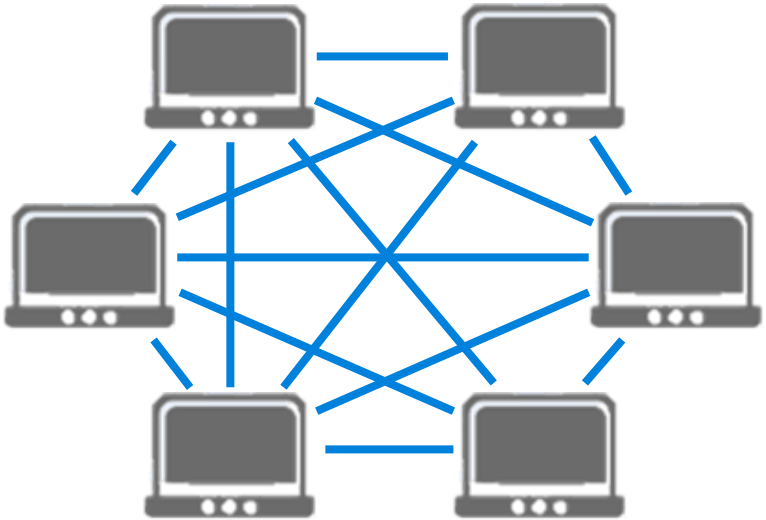
Mejorar el modelo propuesto al identificar variables adicionales que modelen de forma más precisa un ciber-ataque.

Proponer posibles medidas para reducir el impacto o prevenir un ciber-ataque.


Ataques a redes P2P
Definir cuales afectan a este tipo de redes y su clasificación
Cadena infectada
Desarrollo teórico y resolución de una cadena con pares infectados
Redes P2P
Definición y aspectos relevantes
Cadena simple
Desarrollo y resolución de una cadena que refleje una red P2P
Cadena contramedida
Agregar un parámetro que permita disminuir los niveles de infección en la red

Redes de pares-a-pares

Una red Pares-a-Pares (**P2P**) es una **red distribuida** con nodos dinámicos, llamados pares. Los pares en el sistema proporcionan recursos como ancho de banda, espacio de almacenamiento y potencia de cómputo con el objetivo de intercambiar los datos o realizar alguna **tarea colectiva.**



1. Son **más robustas** que las redes sobre servidores ya que los datos se distribuyen en la población.
2. Al haber aumento de demanda también aumenta la capacidad del sistema, **escalabilidad.**

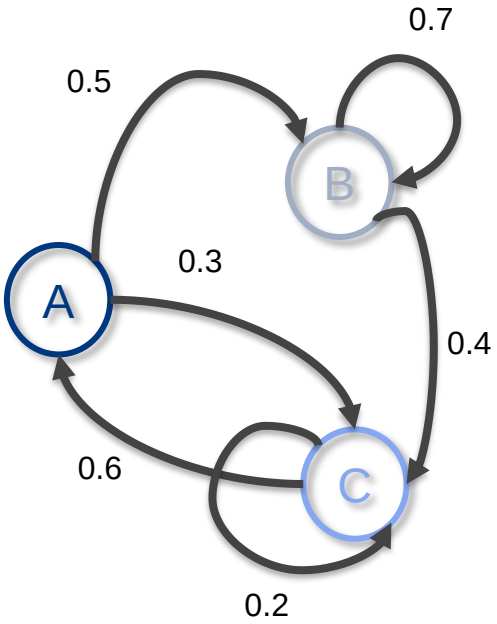
Rivero-Angeles, M. E., & Rubino, G. (2010). Priority-based scheme for file distribution in peer-to-peer networks. *IEEE International Conference on Communications*, 1–6. https://doi.org/10.1109/ICC.2010.5501852

Seguridad en redes P2P

- Las redes P2P no solo son un peligro potencial para los equipos, sino que pueden incurrir en delitos penados.
- Al no existir ningún servidor centralizado que se encargue de subir almacenar y comprobar la autenticidad de los recursos lo que hace que no haya un mecanismo para controlar qué contenido se comparte.

Washbourne, L. (2015) 'A survey of P2P network security', pp. 1–12. Available at: http://arxiv.org/abs/1504.01358.

Cadenas de Markov



- Representa un sistema mediante un conjunto de estados discretos finitos y un conjunto de probabilidades de transición entre estados, se representa usualmente como un grafo dirigido, donde cada uno de los nodos representa un estado del sistema y cada uno de los arcos dirigidos representan las transiciones posibles entre estados.

La evolución en el futuro no depende del pasado, sino solo del estado presente

- Se utilizan comúnmente para representar sistemas que se pueden describir conectados, los cuales son mutuamente excluyentes pero que juntos describen al sistema en su totalidad.

Robayo Santana, E. L. (2009) 'Detección de intrusos en redes de telecomunicaciones IP usando modelos ocultos de Markov / Intrusion detection in IP network telecommunications using hidden Markov models'. Available at: https://repositorio.unal.edu.co/handle/unal/70224 (Accessed: 16 August 2021).
Alberto, J. et al. (2007) Revista Facultad de Ingeniería-Caracterización y simulación del tráfico de redes LAN mediante el modelo MMPP Characterization and simulation of the LAN traffi c by MMPP model, Rev. Fac. Ing. Univ. Antioquia. N. o. Diciembre.

Ataques en redes P2P

- Dos y DDOS
- Hombre en el medio
- Gusanos
- Botnets
- Escuchando a escondidas
- Mascarada

Generales

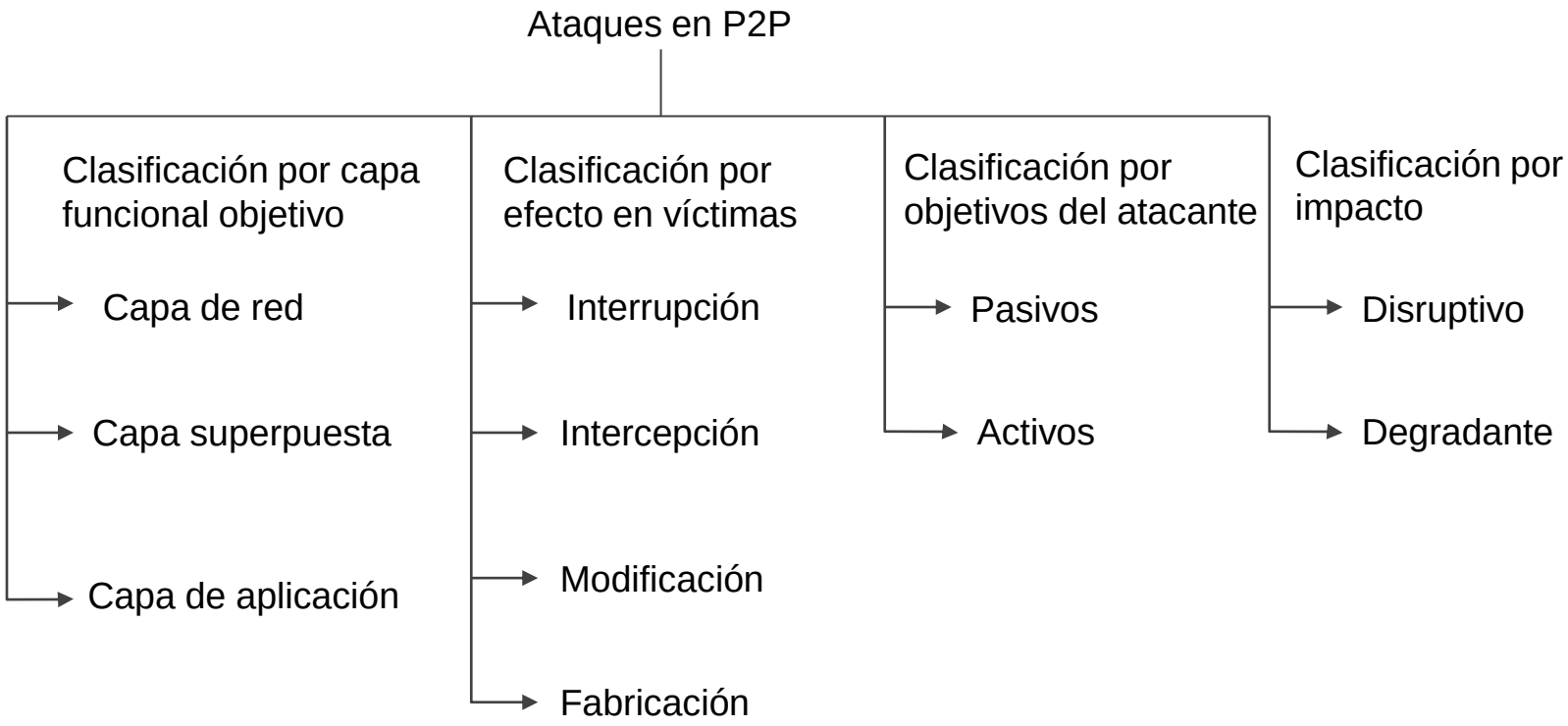
- Sybil
- Mapeo de identidad
- Eclipse
- Robo de identidad
- Churn
- Repetición
- Adivinación
- Cache
- Amplificación de tráfico

Específicos de redes P2P

- Racional
- Almacenamiento
- Envenenamiento
- Contaminación
- Inundación de consultas
- Información de enrutamiento
- Conducción gratuita
- Política y Auditoria

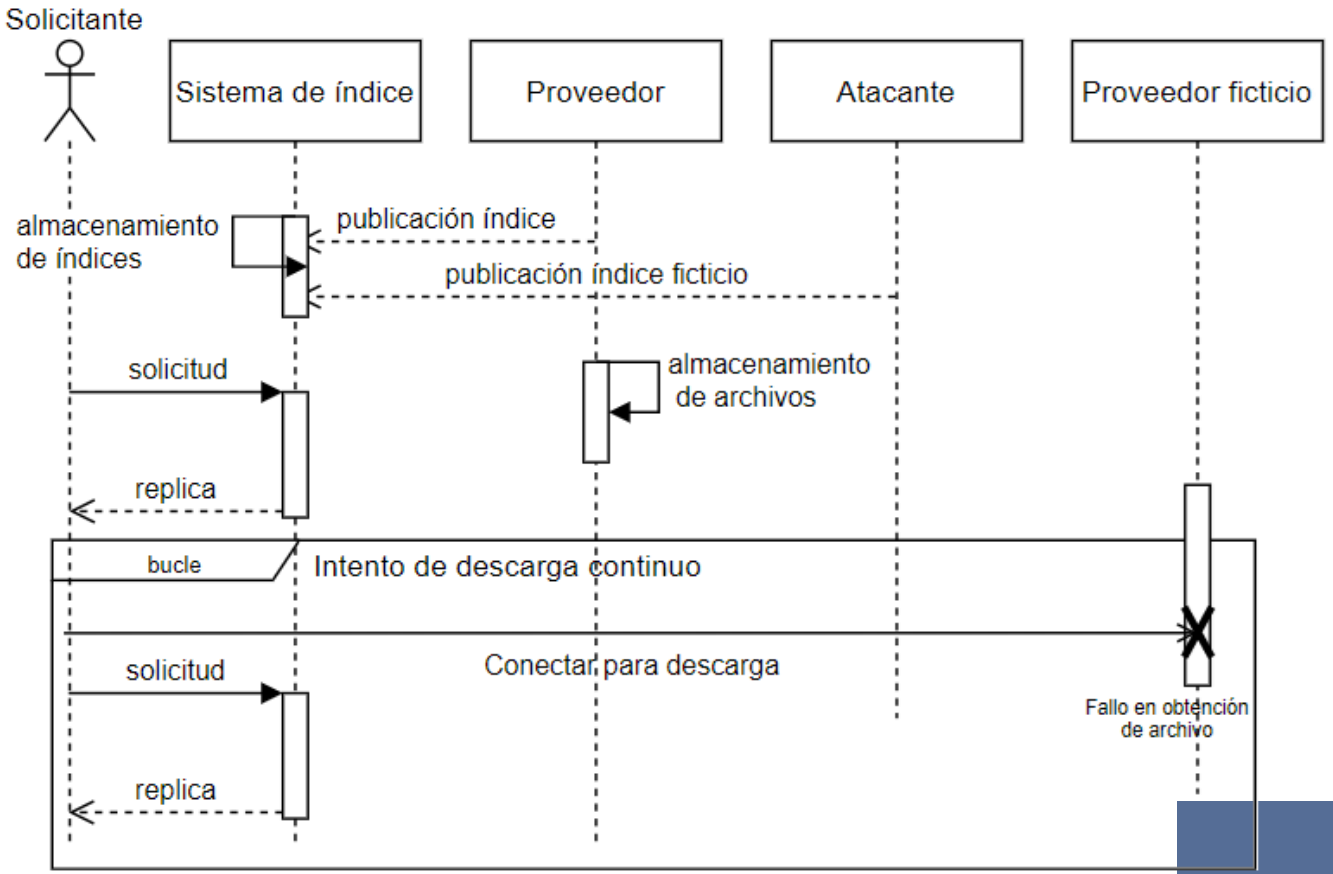
En aplicaciones P2P

Trifa, Z., & Khemakhem, M. (2012). Taxonomy of Structured P2P Overlay Networks Security Attacks. *World Academy of Science, Engineering and Technology*, *6*(4), 460–466.
Ferdous, S., Chowdhury, F., & Moniruzzaman, M. (2007). A Taxonomy of Attack Methods on Peer-to-Peer Network. *Proceedings of the 1th Indian Conference on Computational Intelligence and Information Security*, *2007*(April 2016), 132–138.

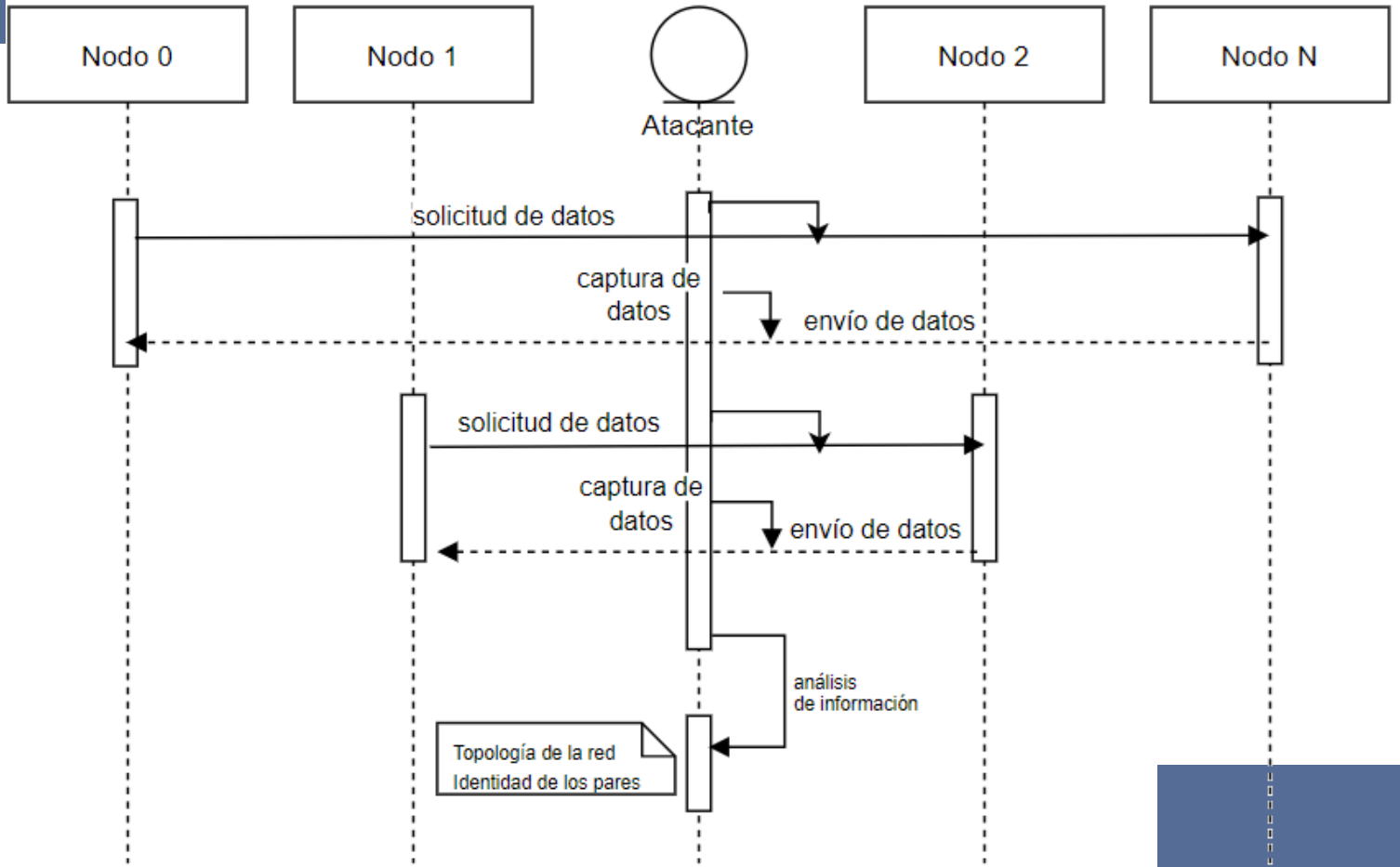


Napster, W. *Security 14*. 319–340. https://doi.org/10.1016/B978-0-12-374214-8.00014-3

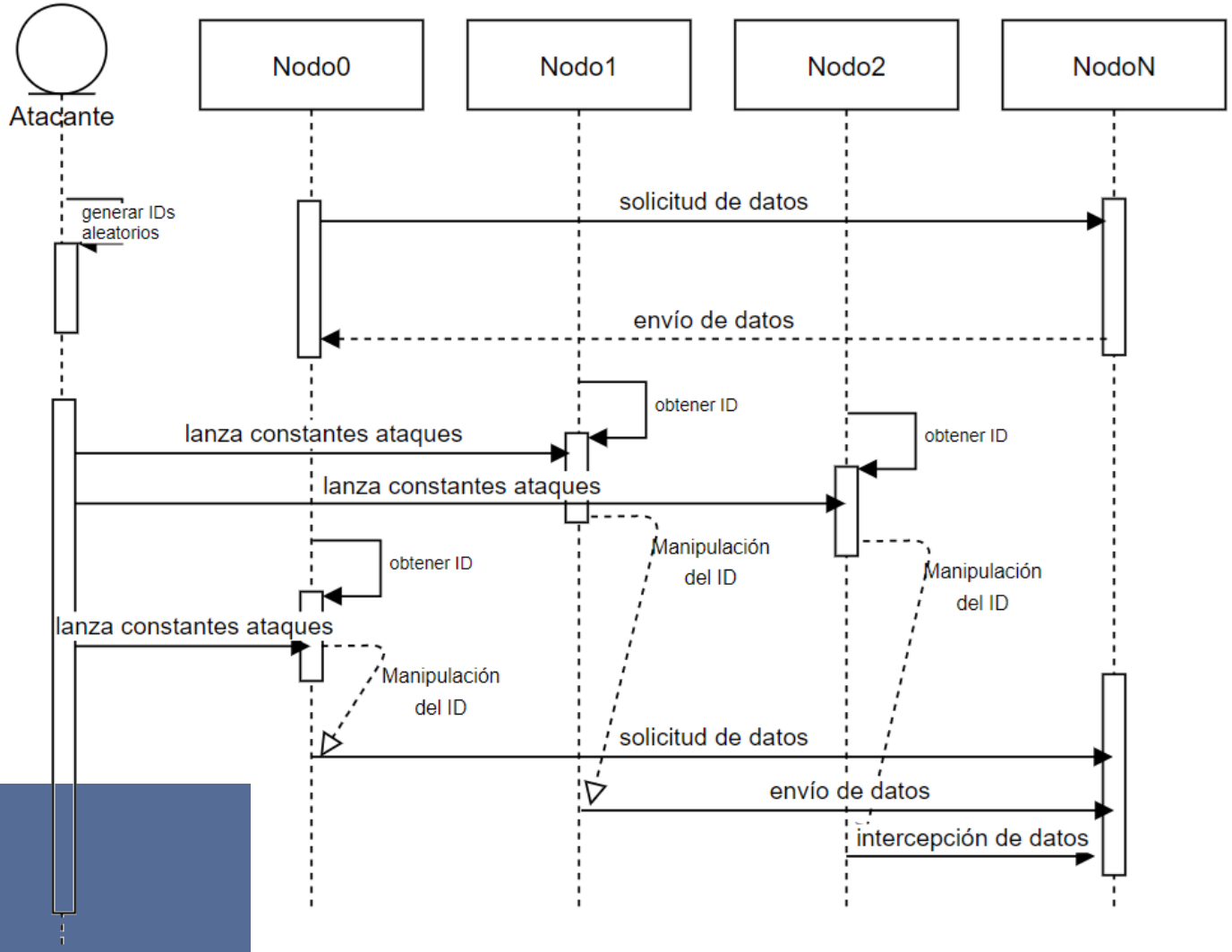
Ataque de envenenamiento



Ataque de análisis de tráfico



Ataques Node Id/ Sybil



Simulación de la cadena simple

Estado inicial

x = 0 = Sanguijuelas
y = 1 = Semillas

Condiciones

Penuria = $M(Nx + y)$
Abundancia = Cx

Parámetros

C = 0.02 (tasa de bajada, archivos/seg)
L = 1 (tasa de arribos, usuarios/seg)
M = 0.00125 (tasa de subida, archivos/seg)
H = 0.01 (tiempo de conexión sanguijuelas, seg)
G = 0.01 (tiempo de conexión semillas, seg)
N = 0.85 (tasa de bajada, archivos/seg)
U = Número aleatorio entre 0 y 1

Operaciones

$$\tau = \min\{M(Nx + y), Cx\}$$

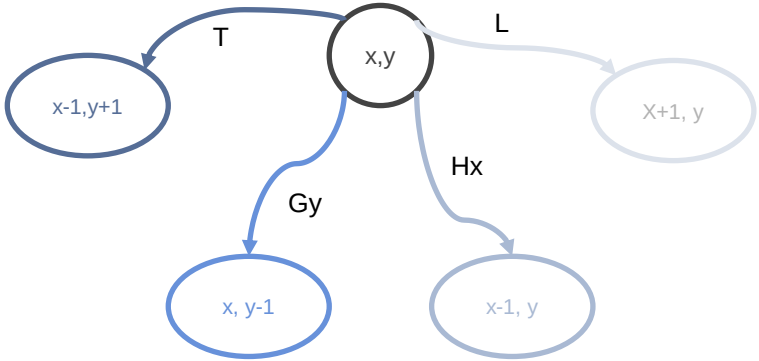
$$T_1 = -\frac{1}{L}\log(1-u)$$

$$T_2 = -\frac{1}{Hx}\log(1-u)$$

$$T_3 = -\frac{1}{Gy}\log(1-u)$$

$$T_4 = -\frac{1}{\tau}\log(1-u)$$

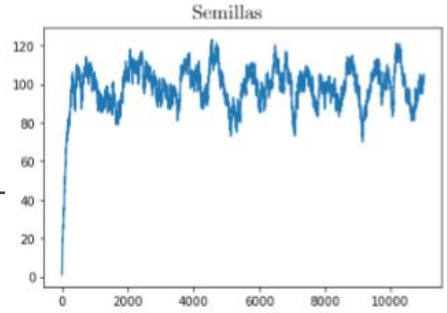
$$T = \min\{T_1, T_2, T_3, T_4\}$$

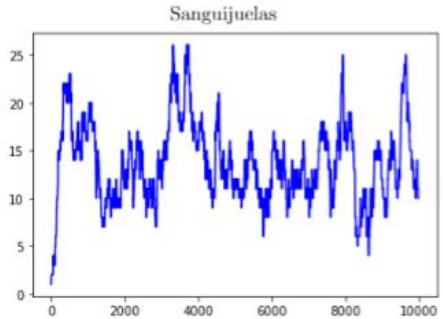


1000000 veces

Sanguijuelas	Semillas
100 ± 15	16 ± 3

$$T_{sim} = \sum_{0}^{100000} T = 89439\ seg \approx 25\ min$$

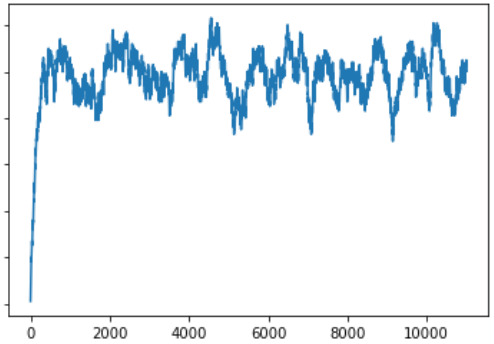


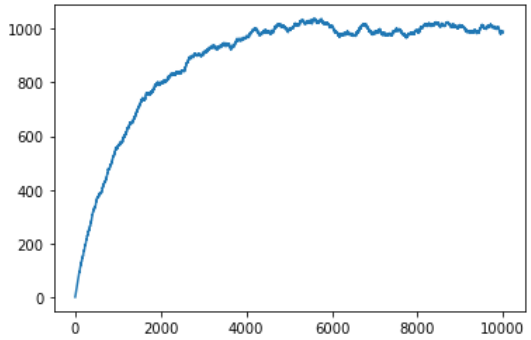


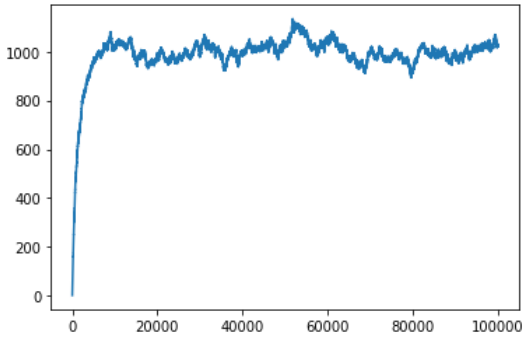
$C = 0.02, \lambda = 1, \mu = 0.00125,$
$\theta = \gamma = 0.01, \eta = 0.85$

$C = 0.002, \lambda = 10, \mu = 0.0005,$
$\theta = \gamma = 0.01, \eta = 0.85$

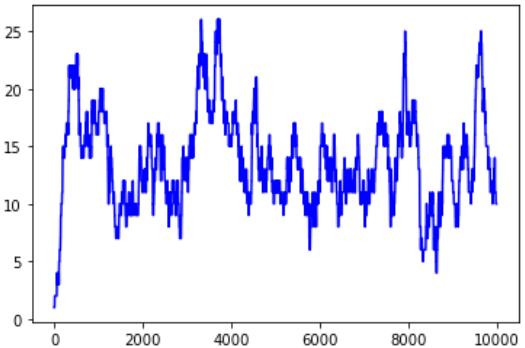
Leeches

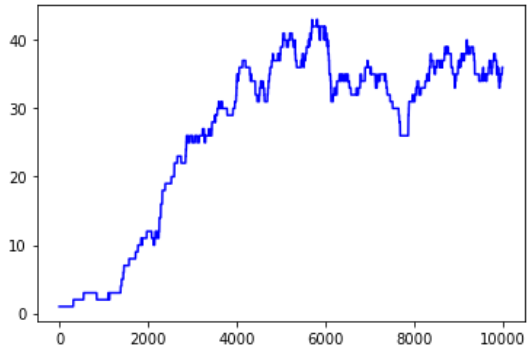


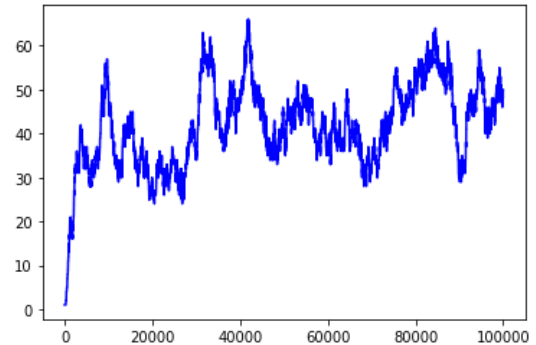




Seeds

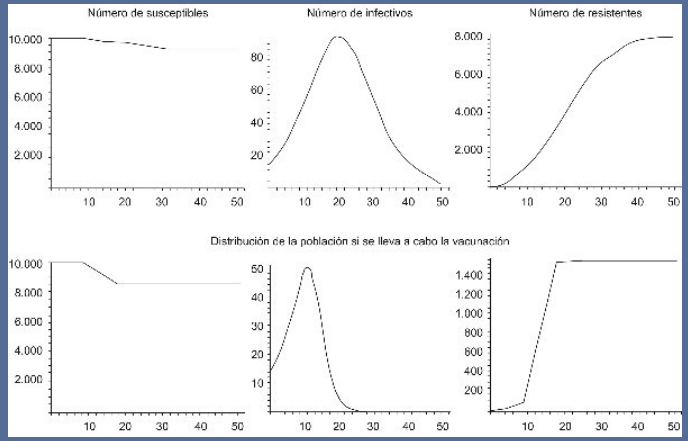






Modelos utilizados comúnmente

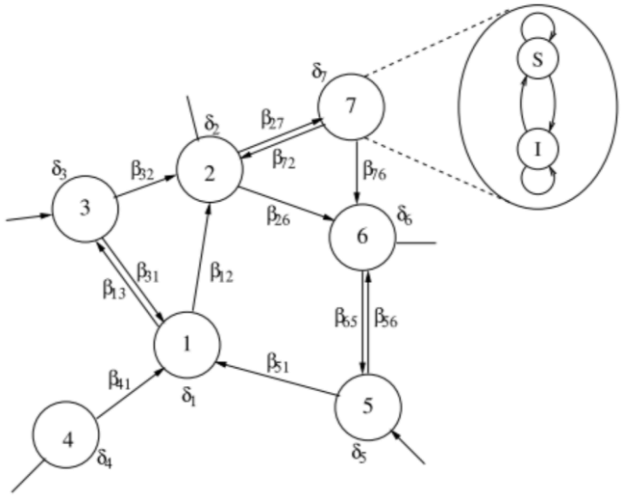
- Modelado a través de la versión modificada de un modelo S-E-I (susceptible-expuesto infectado) de tres estados, utilizando el simulador PeerThing en un modelo de la aplicación Guntella.
- Modelo SEM: modelo de ecuaciones estructurales.
- Modelo SIS: (susceptible-infectado-susceptible).
- Modelo SIR: (susceptible-infectado-recuperado)
- Modelo SIRS: (susceptible-infectado-recuperado-suceptible)
- Modelo ABCD: (Calculo de caja asincrónica con datos) Expresar el comportamiento de sistemas a un alto nivel.

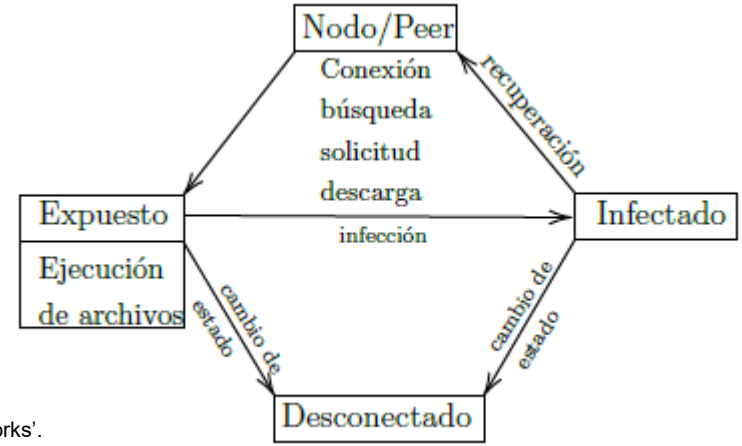


En el caso de la simulación de la propagación de malware, las variables empleadas son el número de dispositivos que se encuentran en alguno de los tipos considerados: susceptibles computadoras, computadoras infecciosas, computadoras expuestas, etc.
Los parámetros habituales utilizados en el modelado son los siguientes:

- la tasa de infección
- la tasa de recuperación
- el número de computadoras retiradas de la red
- las probabilidades de pasar de un compartimento a otro
- la probabilidad de adquisición
- el período de latencia
- el período de inmunidad

El uso de uno u otro depende del modelo implementado y del tipo de malware considerado.

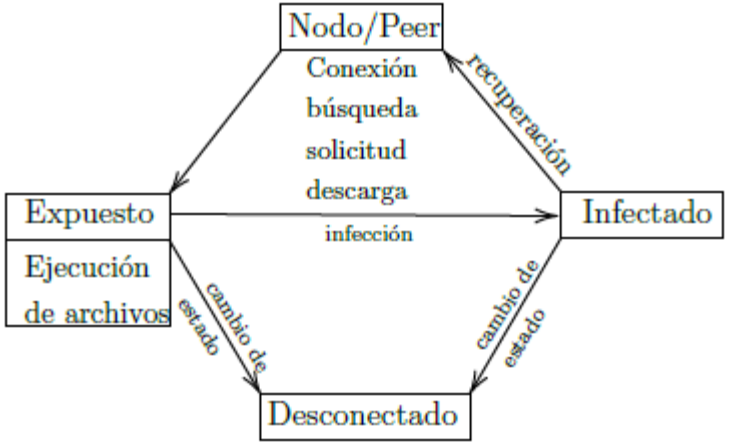


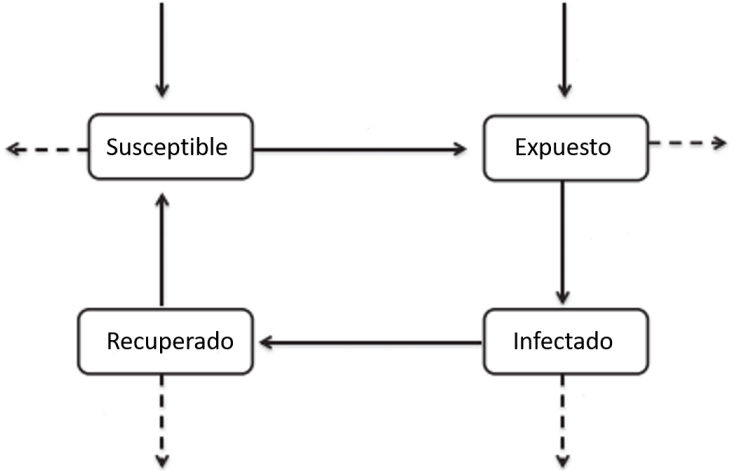


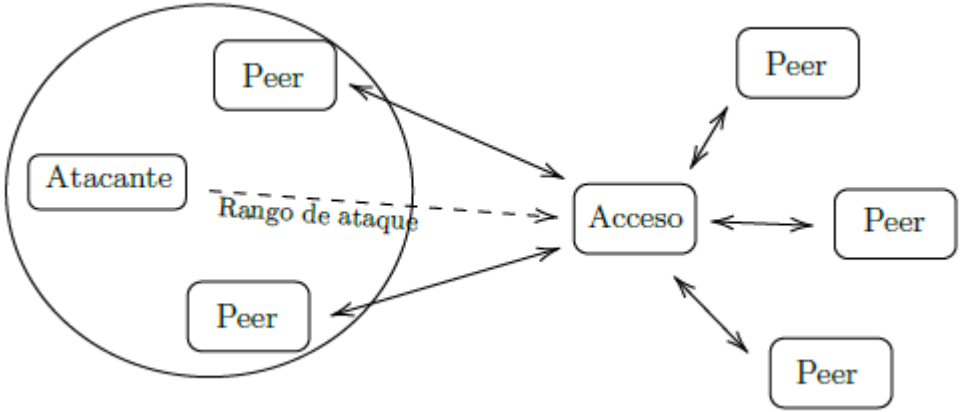
Chen, Z., Member, S. and Ji, C. (no date) 'Spatial-Temporal Modeling of Malware Propagation in Networks'.

Fan, X. and Xiang, Y. (2010) 'Modeling the propagation of Peer-to-Peer worms', Future Generation Computer Systems, 26, pp. 1433–1443. doi: 10.1016/j.future.2010.04.009.

Propagación de archivos infectados







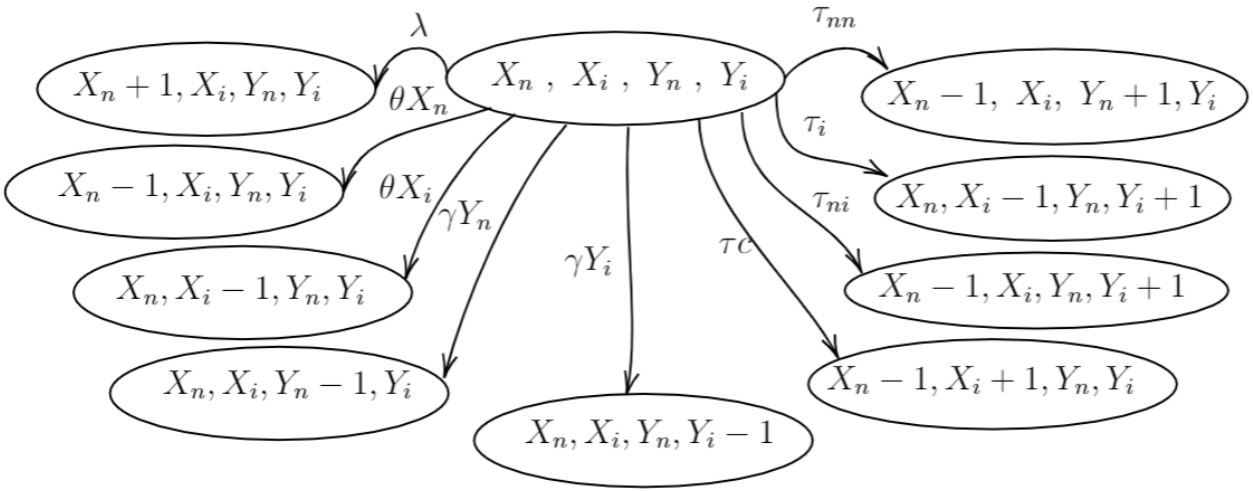
Visualización de la cadena infectada

$X_n \rightarrow$ Sanguijuelas sanas

$X_i \rightarrow$ Sanguijuelas infectadas

$Y_n \rightarrow$ Semillas sanas

$Y_i \rightarrow$ Semillas infectadas



Cadena con nodos sanos e infectados

Estado inicial

x = 0 = Leeches/Sanguijuelas
y = 1 = Seeds/Semillas

Condiciones

Penuria = $M(Nx + y)$
Abundancia = Cx

$$X = x_n + x_i$$
$$Y = y_n + y_i$$
$$P_n = -\frac{x_n N + y_n}{XN + Y}$$

Parámetros

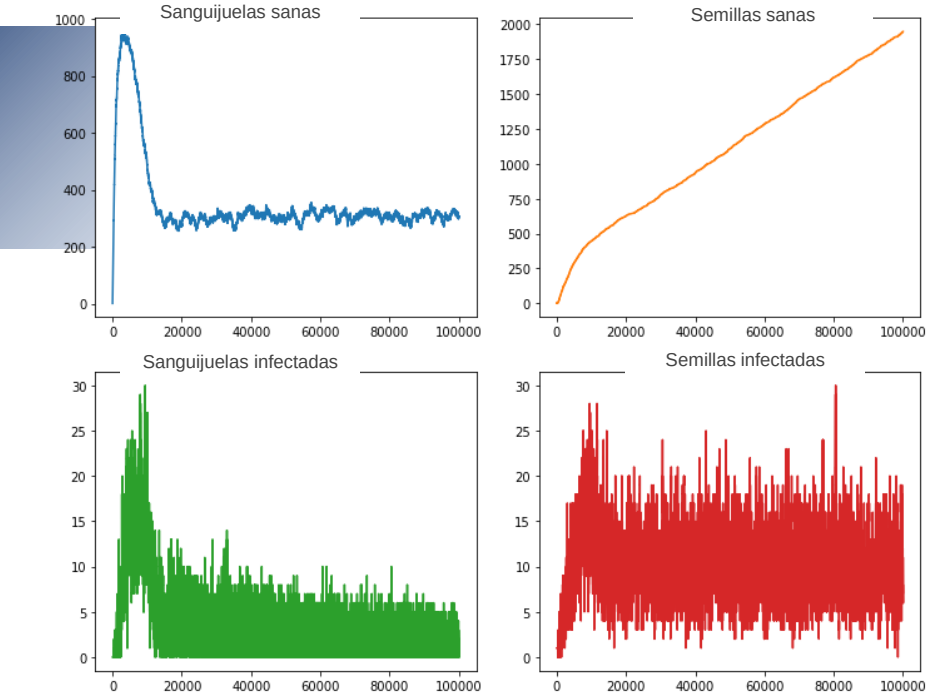
C = 0.002 (tasa de bajada, archivos/seg)
L = 1 (tasa de arribos, usuarios/seg)
M = 0.005 (tasa de subida, archivos/seg)
H = 0.001 (tiempo de conexión sanguijuelas, seg)
G = 0.001 (tiempo de conexión semillas, seg)
N = 0.85 (tasa de bajada, archivos/seg)
K = 1/10 (tasa de chunks, num. trozos/archivos)
U = Número aleatorio entre 0 y 1

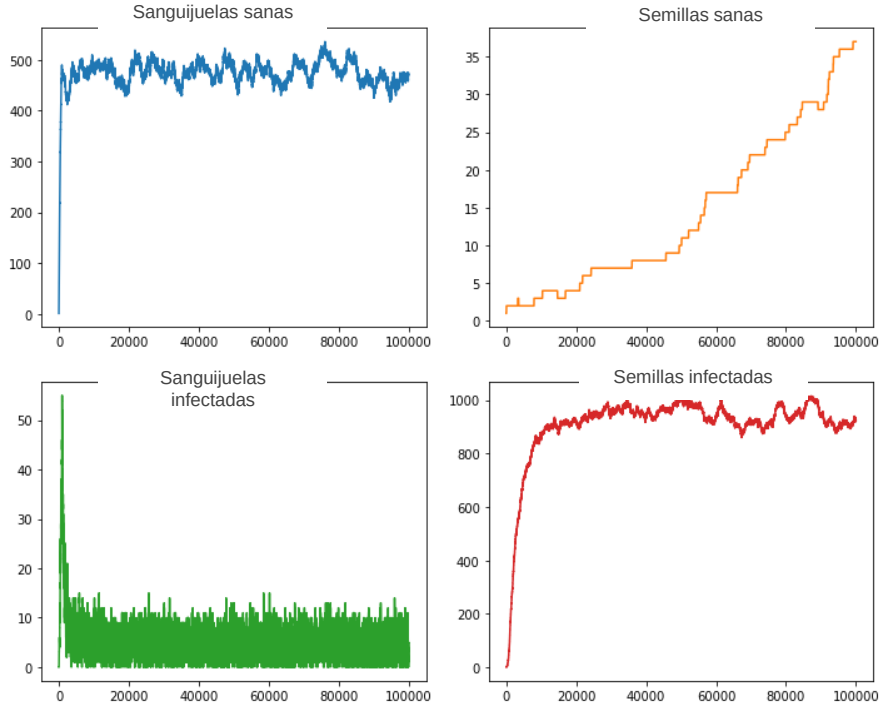
$$\tau = \min\{M(Nx_n + y_n), Cx_n\}$$
$$\tau_i = \text{máx}\{Cx_i, (XN + Y)\}$$
$$\tau_{nn} = \min\{CP_n x_n, M(Nx_n + y_n)\}$$
$$\tau_{ni} = \min\{C(1 - P_n)X_i, M(x_i N + y_n)(1 - P_n)\}$$

Operaciones

$$\tau = \min\{M(Nx + y), Cx\}$$
$$T_1 = -\frac{1}{L}\log(1 - u)$$
$$T_2 = -\frac{1}{Hxn}\log(1 - u)$$
$$T_3 = -\frac{1}{Hxi}\log(1 - u)$$
$$T_4 = -\frac{1}{Gyn}\log(1 - u)$$
$$T_5 = -\frac{1}{Gyi}\log(1 - u)$$
$$T_6 = -\frac{1}{\tau C}\log(1 - u)$$
$$T_7 = -\frac{1}{\tau ni}\log(1 - u)$$
$$T_8 = -\frac{1}{\tau i}\log(1 - u)$$
$$T_9 = -\frac{1}{\tau nn}\log(1 - u)$$
$$T = \min\{T_1, T_2, T_3, T_4, T_5, T_6, T_7, T_8, T_9\}$$

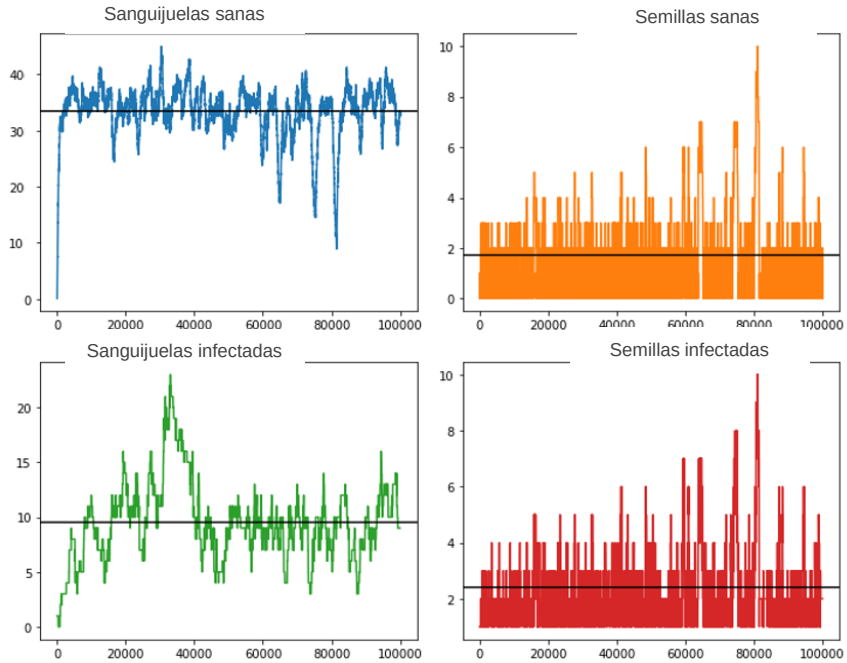
Gráficas de la cadena infectada





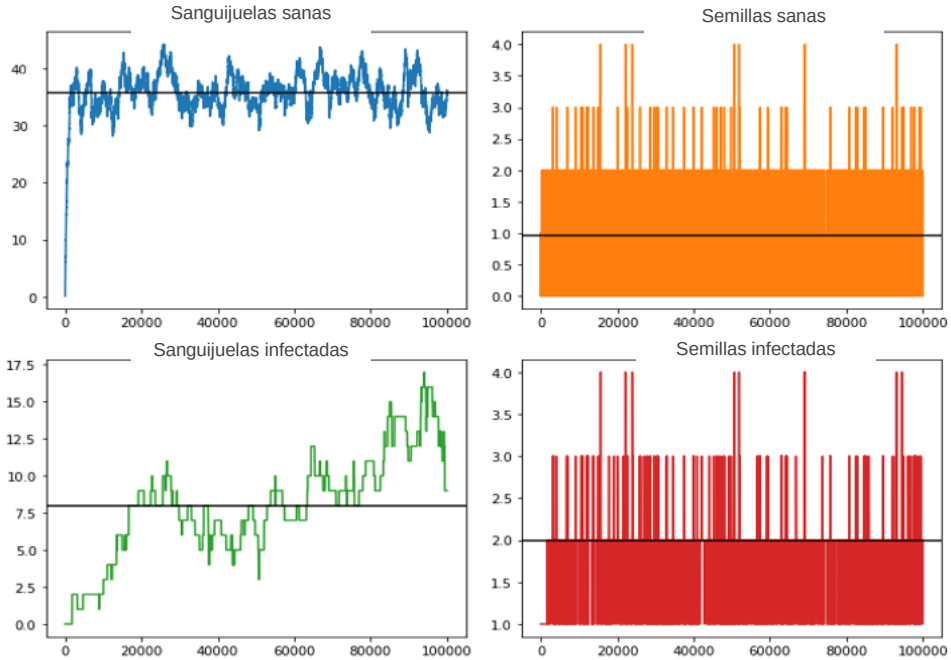
Pequeñas variaciones en los parámetros de la cadena provocan gran variación en el número de peers que aparecen pero el comportamiento es similar en los distintos casos para cada etiqueta de los nodos.

Sanguijuelas sanas: 33.419332
Semillas sanas: 1.72068
Sanguijuelas infectadas: 9.4831
Semillas infectadas: 2.3969



Reducción en las variables

Sanguijuelas sanas: 35.994569
Semillas sanas: 0.96869
Sanguijuelas infectadas: 7.99186
Semillas infectadas: 1.98949

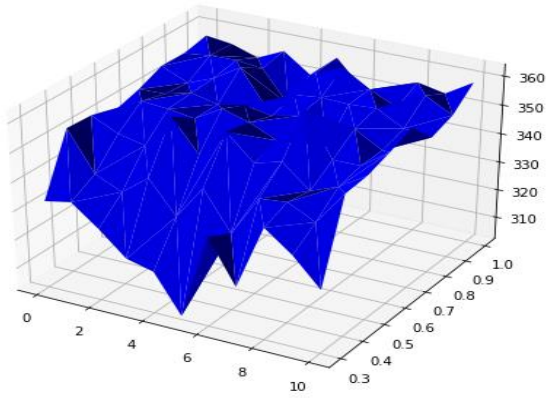


Variación de las tasas de los estados para limitar el aumento de seeds sanos.

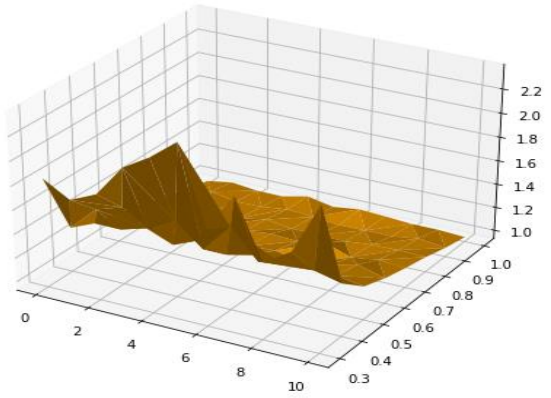
G

Promedio de cada uno de los grupos variando el número de nodos infectados inicialmente y el parámetro de Gamma

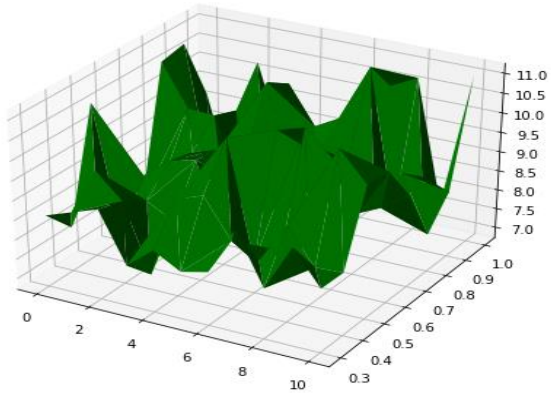
Sanguijuelas sanas



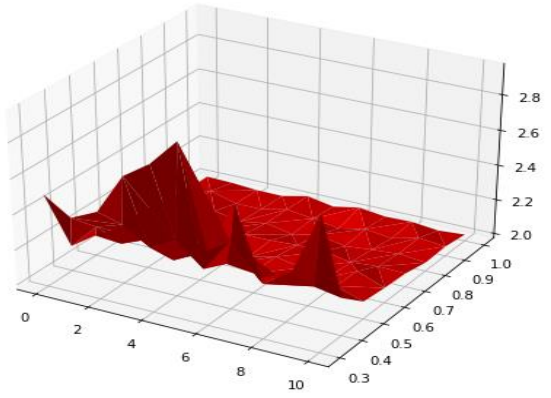
Semillas sanas



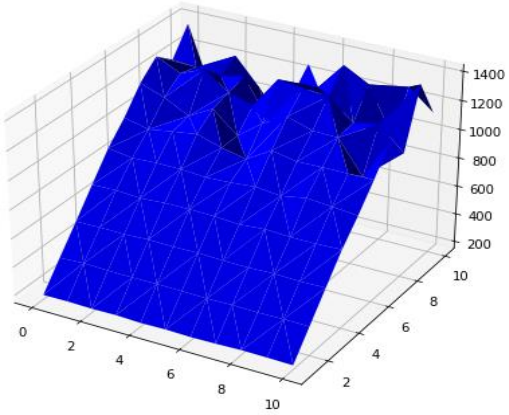
Sanguijuelas infectadas



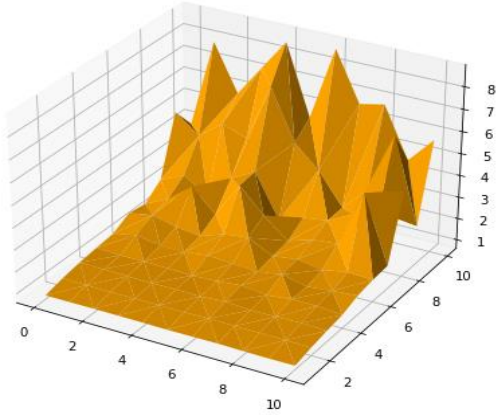
Semillas infectadas



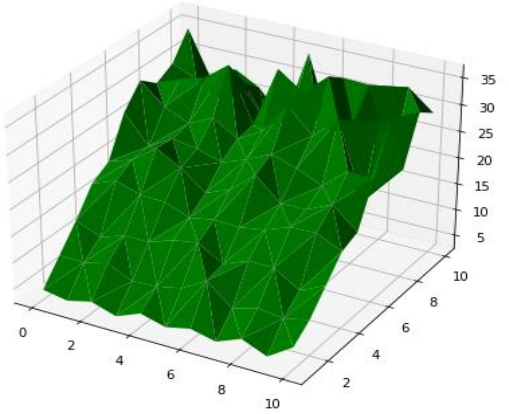
Sanguijuelas sanas



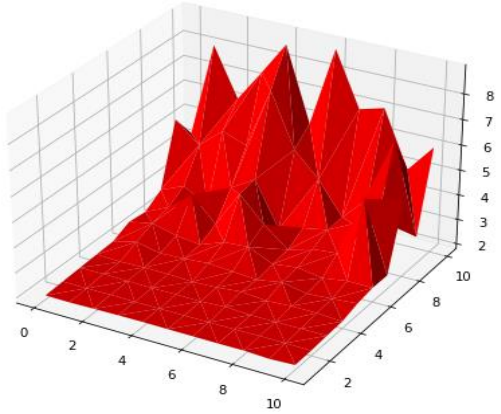
Semillas sanas



Sanguijuelas infectadas



Semillas infectadas



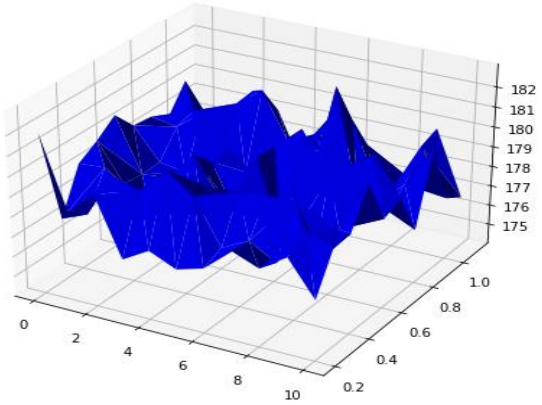
L

Promedio de cada uno de los grupos variando el número de nodos infectados inicialmente y el parámetro L

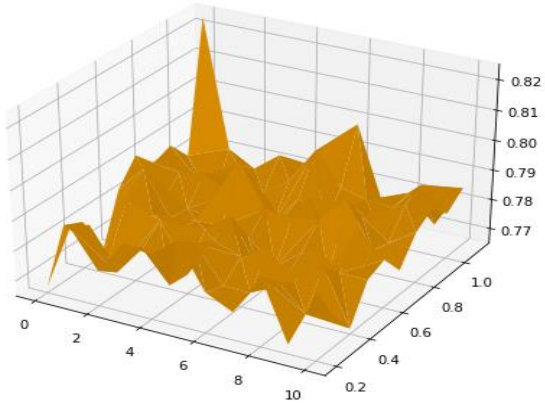
N

Promedio de cada uno de los grupos variando el número de nodos infectados inicialmente y el parámetro de N

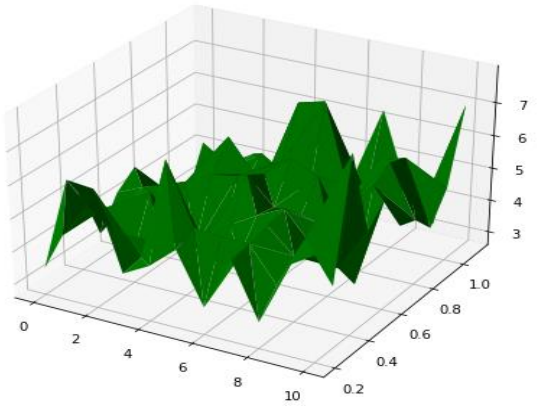
Sanguijuelas sanas



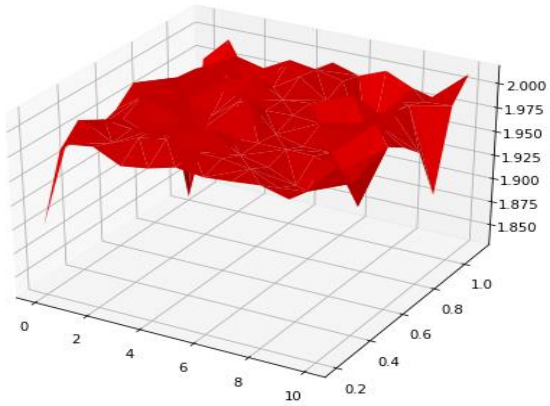
Semillas sanas



Sanguijuelas infectadas

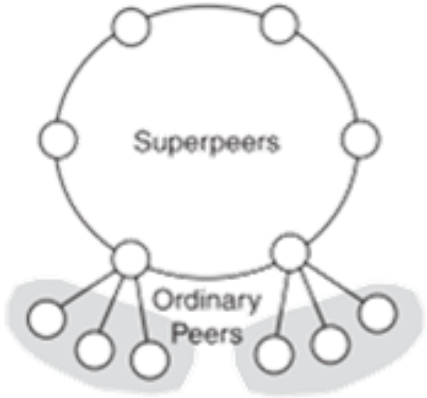


Semillas infectadas



MECANISMOS DE SEGURIDAD

- Soluciones Criptográficas
- Limitación de velocidad y filtrado
- Autoridades de certificación centralizados
- Arquitecturas P2P híbridas
- Equidad en el intercambio de recursos
- Protección contra virus y el filtrado de archivos

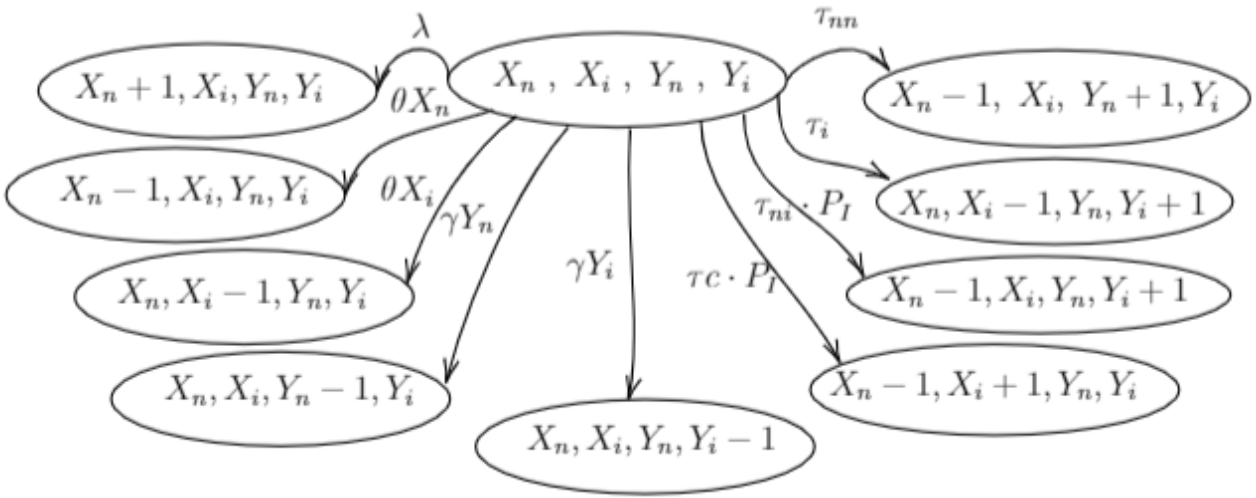


Métodos de seguridad

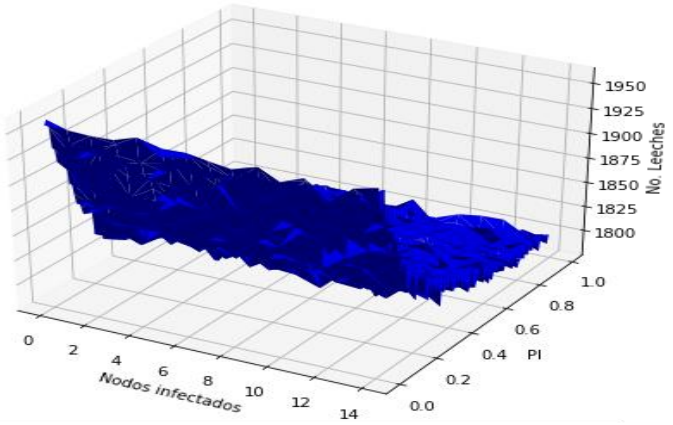
Nombre	Objetivo	Mecanismo
ARAN	Autenticación, integridad y no repudio de paquetes de señalización.	Certifica autoridad y marcas de tiempo.
ARIADNE	Autenticación, integridad de paquetes de señalización.	Criptografía simétrica, funciones hash y marcas de tiempo
CONFIDANT	Excluir mal comportamiento	Sistema de reputación
DCMD	Detecta y corrigen datos malicioso	Observación y plausibilidad de eventos
SAODV	Autenticación, integridad de paquetes de señalización.	Digitalización de firmas y cadenas hash.
SEAD	Autenticación, integridad de paquetes de señalización.	Cadenas hash u secuencia de números
SLSP	Autenticación, integridad y no repudio de paquetes de señalización.	Certificación de autoridad
SPAAR	Autenticación, integridad y no repudio de paquetes de señalización.	Certificación de autoridad y marcas de tiempo
SOLSR	Autenticación, integridad de paquetes de señalización.	MACs y marcas de tiempo
WATCHDOG	Excluir mal comportamiento	Observación y reputación

Mihaita, A., Dobre, C., Mocanu, B., Pop, F., & Cristea, V. (2015). Analysis of Security Approaches for Vehicular Ad-Hoc Networks. *Proceedings - 2015 10th International Conference on P2P, Parallel, Grid, Cloud and Internet Computing, 3PGCIC 2015*, 304–309. https://doi.org/10.1109/3PGCIC.2015.184

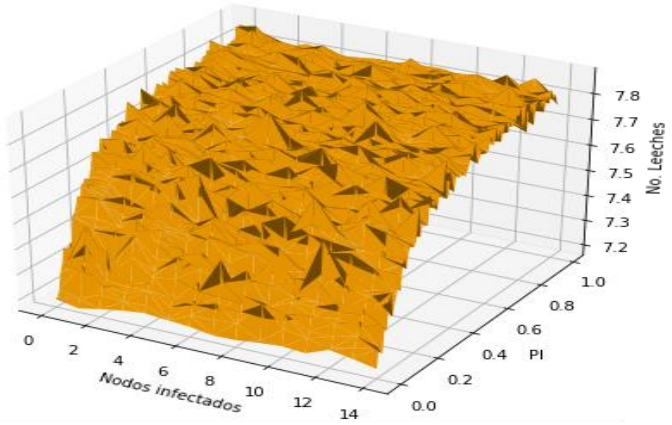
Visualización de la cadena infectada + contramedida



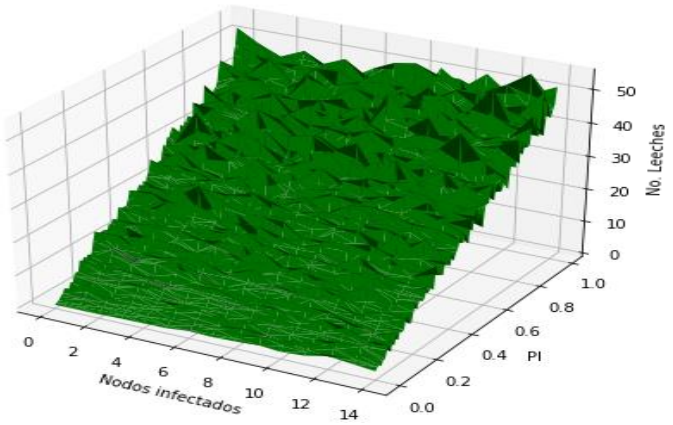
Sanguijuelas sanas



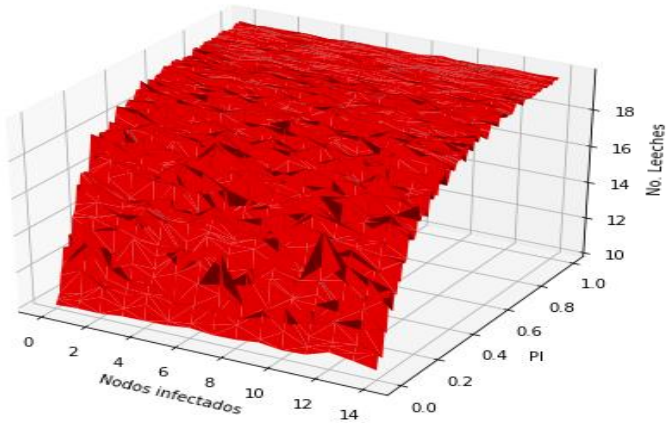
Semillas sanas



Sanguijuelas infectadas



Semillas infectadas



Cadena + PI

Conclusiones

Se analiza en términos de una cadena de Markov, el comportamiento de las redes de pares a pares de una manera sencilla en tres escenarios distintos.

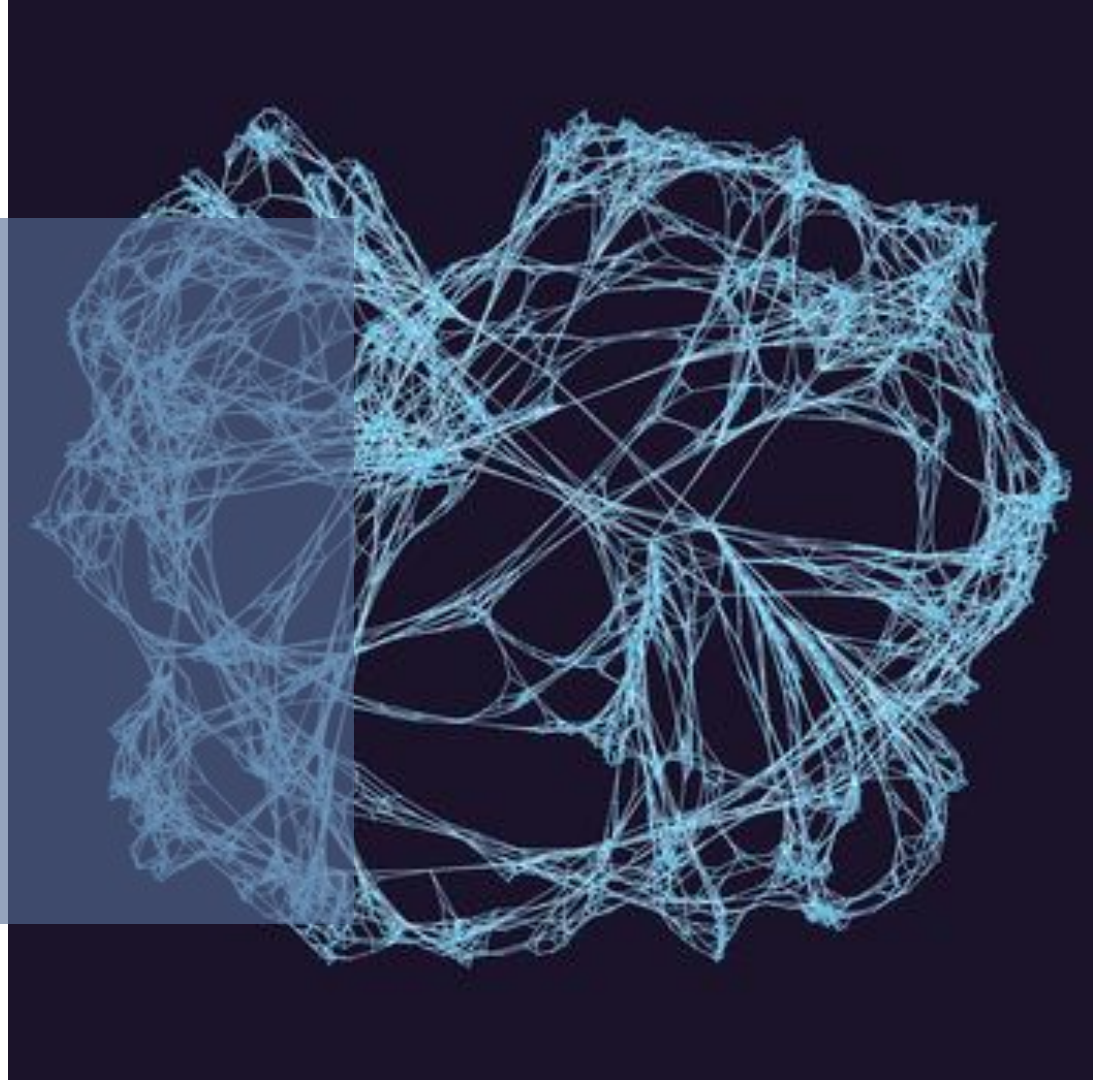
El primero, el funcionamiento normal de una red P2P, donde se observó que después de 100,000 iteraciones ya se llega a un estado estable.

En segundo, la red ya probada que converge a un estado se le aumentan parámetros, esto ocasiona el surgimiento de un nuevo tipo de pares infecciosos invadiendo el sistema, desestabilizando la red y afectando el posible crecimiento o conexión de los pares sanos.

Finalmente, se adicionó un parámetro para conocer el impacto de posibles medidas de seguridad, ya sea a nivel de red o a nivel usuario.

De acuerdo a los objetivos planteados, se logró completar el esquema simple del sistema, analizando su comportamiento bajo distintas condiciones, identificando en cuales de estas condiciones la red se encuentra más vulnerable y cuál es la causa de la debilidad.

¡Gracias por su atención!



REFERENCIAS

- ESQUIVEL, E. B. y col.: Priority scheme for window-based video-on-demand transmissionon BitTorrent-like Peer-to-Peer networks. En:2013 IEEE International Conference onCommunications (ICC). 2013, págs. 3000-3005.
- ROBAYO SANTANA, E. L.: Detección de intrusos en redes de telecomunicaciones IPusando modelos ocultos de Markov/Intrusion detection in IP network telecommunicationsusing hidden Markov models.Departamento de Ingenierıa de Sistemas e Industrial. 2009.
- TORRES-CRUZ, N. y col.: An efficient resource allocation scheme for VoD services overwindow-based P2P networks.Multimedia Tools and Applications. 2018, vol. 77, n.o23,págs. 31427-31445.
- BOCEK, T. y col.: Game theoretical analysis of incentives for large-scale, fully decentra-lized collaboration networks. En:2008 IEEE International Symposium on Parallel andDistributed Processing. 2008, págs. 1-8.
- TOSUN, U.:Hidden Markov models to analyze user behaviour in network traffic. 2005.Inf. téc. Citeseer.
- SUÑÉ TORRENTS, A. y col.:Cadenas de markov: Métodos cuantitativos para la toma dedecisiones III. Universitat Politècnica de Catalunya. Iniciativa Digital Politècnica, 2017.
- QIU, D. y SRIKANT, R.: Modeling and performance analysis of BitTorrent-like peer-to-peer networks.ACM SIGCOMM computer communication review. 2004, vol. 34, n.o4,págs. 367-378.
- KESIDIS, G. y col.: A stochastic epidemiological model and a deterministic limit forBitTorrent-like peer-to-peer file-sharing networks. En:International Conference on NetworkControl and Optimization. 2008, págs. 26-36.
- Deng, L., He, Y., & Xu, Z. (2009). Combating index poisoning in P2P file sharing. Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 5576 LNCS(90818012), 358–367. https://doi.org/10.1007/978-3-642-02617-1_37
- Dinger, J., & Hartenstein, H. (2006). Defending the sybil attack in P2P networks: Taxonomy, challenges, and a proposal for self-registration. Proceedings - First International Conference on Availability, Reliability and Security, ARES 2006, 2006, 756–763. https://doi.org/10.1109/ARES.2006.45