Ataques en Redes P2P

1. Ataques generales a redes

   a) DoS y DDoS: Causan que el servicio dejen de funcionar al utilizar solicitudes de servicio razonables para agotar los recursos del host objetivo. Disponibilidad. Defensa: Pricing. El host envía acertijos a sus clientes antes de continuar con el cálculo solicitado, asegurando así que el cliente realice un cálculo igualmente costoso.

   b) Man in the middle(MiTM): Un atacante se inserta entre otros dos nodos de la red, realiza conexiones independientes y transmite mensajes entre ellos. Confidencialidad, integridad. Defensa: uso de firmas digitales basadas en criptografía de clave pública.

   c) Worms: Pieza de software complejo que es capaz de ataques mucho más complicados, como la recopilación de todo tipo de información. Confidencialidad. Defensa: actualizaciones de seguridad periódicas.

   d) Botnets: redes de máquinas comprometidas bajo el control de un atacante. No repudio. Defensa: dividir nodos de alto grado para evitar respuestas específicas y diseñar conjuntos de pruebas de turing.

   e) Eavesdropping: Los atacantes pueden obtener acceso a los datos dentro de una red y espiar el tráfico. Confidencialidad. Defensa: fuerte seguridad física y fuertes servicios de encriptación.

   f) Masquerade: Una entidad del sistema se hace pasar ilegítimamente como otra entidad para obtener acceso a sistemas confidenciales. Confidencialidad, Autenticación, integridad. Defensa: filtrar los paquetes entrantes que parecen provenir de una dirección IP interna o de una dirección invalida.

2. Ataques específicos a redes P2P

   a) A nivel de red

      1) Sybil: El usuario malintencionado puede crear múltiples identidades falsas y pretender ser múltiples nodos físicos distintos en el sistema y atacan varios protocolos, como el almacenamiento distribuido para anular los mecanismos de replicación y fragmentación. Autenticación. Defensa: El sistema debe garantizar que las identidades distintas se refieran a entidades distintas y limitar la capacidad de una entidad para determinar la identidad.
      2) ID mapping: Permite a un atacante obtener algún identificador particular y ganar una posición estratégica en la red para ganar control sobre ciertos

recursos. Defensa: el identificador depende de algún dato fuera del control de un nodo.

3) Eclipse: El atacante genera una gran cantidad de identidades falsas y colocar esas identidades en la red para mediar en la mayor parte del tráfico y eclipsar los nodos correctos. Autenticación. Defensa: firmas digitales y criptografía de clave pública.
4) Robo de identidad: El nodo malicioso en la ruta de un mensaje afirma que es el nodo de destino deseado, por lo que puede secuestrar solicitudes de ruta y búsqueda para falsificar y destruir datos. Defensa: utilizar pruebas, listas negras.
5) Churn. se generan peers que se unen y abandonan la red lo suficientemente rápido como para corromper la mejor función de la red.Disponibilidad. Defensa: diseño que pueda manejar de manera eficiente la gran cantidad de pares que se unen al sistema durante solo unos minutos.
6) Replay: una transmisión de datos válida es maliciosa o fraudulentamente repetida, un adversario intercepta la información y la retransmite, posiblemente como parte de un ataque enmascarado. Integridad, confidencialidad, autenticación. Defensa: uso de la marca de tiempo para evitar que el P2P inalámbrico sufra ataques malintencionados.
7) Guessing: El atacante intercepta mensajes de dos usuarios legales para obtener la contraseña de un usuario. Confidencialidad, autenticación. Defensa: la contraseña de un usuario se verifica localmente y no es necesario transmitirla en el canal.
8) Cache Data: Aunque los cachés ofrecen un aumento del rendimiento, pueden ser explotados por atacantes y crear un degradamiento de la red.
9) Traffic Amplification: magnifica el efecto de un solo host atacante, un solo host atacante aparece como múltiples hosts y puede tirar redes enteras. Disponibilidad.

b) A nivel aplicación

1) Racional: El nodo intentará maximizar su consumo de recursos del sistema mientras minimiza el uso de los suyos. Disponibilidad. Defensa: sistema de trueque por fragmentos de datos, cuanto más comparta un nodo con otros, más recibirá.
2) Storage and retrival: los usuarios malintencionados se niegan a prestar servicios a los demás nodos o niegan la existencia de datos de los que eran responsables. Disponibilidad, no repudio. Defensa: El sistema debe garanti-

zar la replicación, de manera que ningún nodo sea responsable de facilitar el acceso a las réplicas.

3) Poisoning: Inyecta una gran cantidad de señuelos o archivos que no se pueden leer en la red. Disponibilidad, integridad. Defensa: descargar versiones de esos anuncios y luego intentar determinar si las versiones de descarga están limpias o envenenadas.
4) Pollution: El atacante corrompe el contenido del archivo compartido, dejándolo inutilizable y reenvía el archivo dañado a otros pares. Disponibilidad, integridad. Defensa: listas negras, cifrado de tráfico, verificación hash, firma de fragmentos y detección sin descargar.
5) Query flooding: El nodo malicioso genera tantas consultas como sea posible para inundar la red y no se puede establecer la sesión de descarga. Disponibilidad. Defensa: después de obtener el número máximo de consultas simplemente elimina el resto de solicitudes.
6) Routing information: El nodo malicioso reenvía las consultas al nodo incorrecto o inexistente y luego el nodo original puede que nunca encuentre el nodo de destino. Disponibilidad.
7) Free Riding: hay pares consume principalmente recursos y produce muy pocos, ya sea no compartir contenido o recursos computacionales.
8) Policy, Auditing: Explotan vulnerabilidades en las políticas de la red y los sistemas de auditorías y que no detecten comportamientos extraños. Autenticación.

Mecanismos y métodos de seguridad

1. ARAN: (Authenticated Routing for Ad hoc Net- works) Cada usuario debe obtener un certificado para poder ingresar a la red, que debe estar basada en IP. Des: no escalable.

2. ARIADNE: 3 versiones: secreto compartido entre cada par de nodos, entre nodos de comunicación combinados con autenticación de difusión o firma digital. Des: Incrementa longitud de paquetes.

3. CONFIDANT: (Cooperation Of Nodes: Fairness In Dynamic Ad hoc NeTworks) Detección de nodos maliciosos monitoreando constantemente el estado de los mensajes en la red y los informes sobre los ataques. Des: poca escalabilidad.

4. DCMD: (Detecting and Correcting Malicious Data in VANET): En función de los datos recopilados de los sensores para determinar la exactitud de la información recibida y, por lo tanto, detectar nodos maliciosos. Des; no se puede asegurar la integridad de la información de los sensores.

5. SAODV(Secure Ad hoc on demand Distance Vector) dividir los mensajes en campos modificables que están firmados y campos fijos que se transmiten a través de su hash. Des: depende de los recursos.

6. SEAD(Secure Efficient Ad hoc Distance Vector) Funciones hash unidireccionales del mensaje para garantizar la integridad. Des: Necesita pasos adicionales de seguridad.

7. SLSP(Secure Link State routing Protocol) usa funciones hash y criptografía de clave pública para asegurar el enrutamiento de mensajes. Des: consume muchos recursos.

8. SPAAR(Secure Position Aided Ad hoc Routing) proporciona autenticación, integridad de mensajes, no repudio de los mensajes enviados y confidencialidad. Des: toma el doble de tiempo computar mensajes.

9. SOLSR(Secure Optimized Link State Routing) utiliza MAC hash unidireccionales para otorgar autenticación y evitar ataques de respuesta. Des: problemas de escalabilidad.

10. WATCHDOG-PATHRATER monitorea la red para detectar nodos que se comportan mal, y encontrar rutas alternativas para evitar nodos maliciosos. Des: mucho tiempo para intercambiar mensajes.

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

Algoritmos de encriptación simétrica

1. Advanced Encryption Standard (AES): 3 versiones basadas en longitudes de clave 128, 192 y 256 bits; la longitud, a su vez, determina el número de rondas de cifrado (que pueden ser 10, 12 y 14), utiliza operaciones como sustitución-permutación, que son rápidas tanto en hardware como en implementación de software.

2. AES Fast: 8 KB de tablas estáticas para almacenar cálculos redondos precalculados. Cada tabla tiene tablas de 4256 palabras, que se utilizan para el cifrado, y tablas de 4 palabras que se utilizan para la fase de descifrado.

3. AES Light: No tiene tablas estáticas y, por lo tanto, es la versión más lenta del algoritmo AES.

4. Blowfish: The algorithm has 16 rounds, and uses block sizes of 64-bits and keys with variable length between 32 bits and 448 bits. Rápido.

5. Twofish: Tiene 16 rondas y puede admitir tres posibles tamaños de bloque de claves de 128, 192 y 256 bits, con bloques de datos de 128 bits, usa S-boxes precalculados dependientes de la clave, y un programa de claves complejo.

6. Camellia: Tiene 18 o 24 rondas, y tres posibles dimensiones de clave de 128, 192 y 256 bits, con bloques de datos fijos de 128 bits. Comparable al AES.

7. Tiny Encryption Algorithm (TEA): Tiene un número variable de rondas, aunque se recomiendan 64 rondas. Utiliza un tamaño de bloque de 64 bits y tamaños de clave de 128 bits.

$$\tau = \min(M(Nx + y), Cx)$$
$$T_1 = -\frac{1}{L}\log(1-u)$$
$$T_2 = -\frac{1}{Hx}\log(1-u)$$
$$T_3 = -\frac{1}{Gy}\log(1-u)$$
$$T_4 = -\frac{1}{\tau}\log(1-u)$$
$$T = \min(T_1, T_2, T_3, T_4)$$

Propagación de virus

- Swen: Se propaga a través de correo, hace copias de si mismo y se comparte, puede ocultarse del parche de Microsoft, pide información confidencial con mensajes falsos.

- Fizzer: Se propaga a través de correo, puede contener puertas traseras y key loggers, ver información confidencial y desactivar el anti-virus.

- Lirva: Se envía a si mismo por correo y desactiva firewalls y anti-virus.

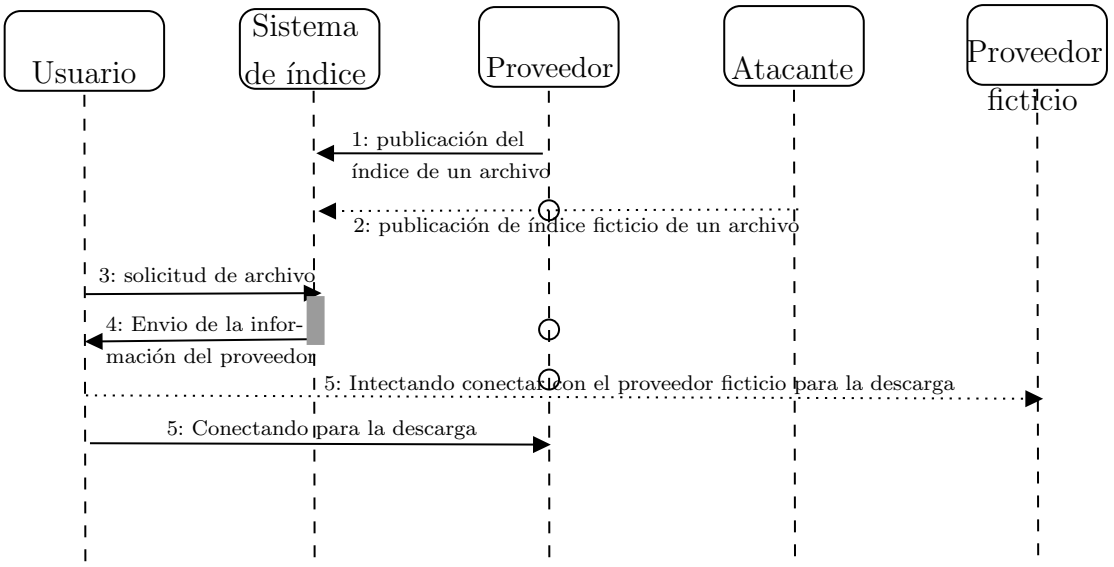

Figura 1: Ataque de envenenamiento de índice

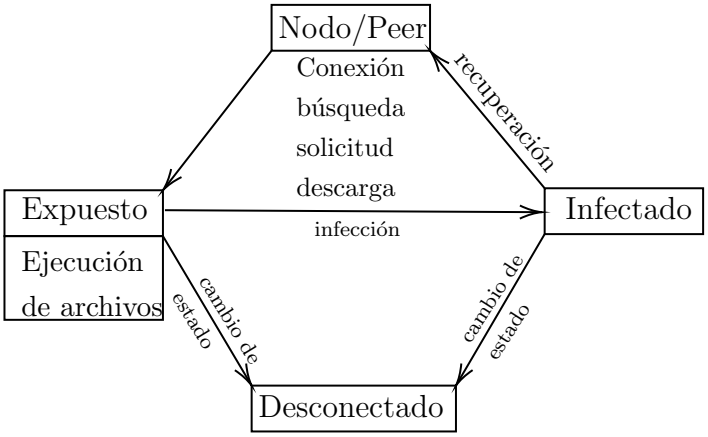

Figura 2: Propagación de un virus

- Magic Eightball: Virus troyano, elimina archivos y despliega cuadros de dialogo.
- Benjamin: Falsos mensajes de error, se copia a sí mismo y se coloca en folders compartidos.
- Lolo.a: Rutina de puerta trasera que se conecta al canal IRC ejecutando comandos del autor.

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)

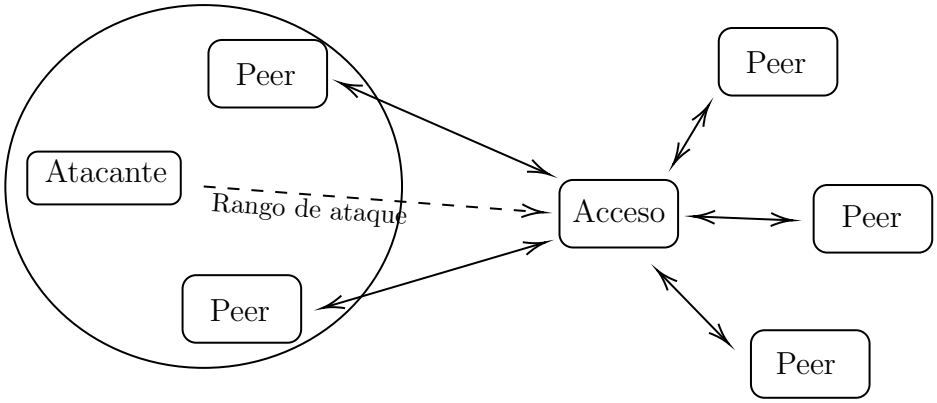

Figura 3: Ataque a pares a través de un punto de acceso

Modelo SIR: (susceptible-infectado-recuperado-suceptible)

Modelo ABCD: Cálculo de caja asincrónica con datos) Expresar el comportamiento de sistemas a un alto nivel.

Botnets

- Mecanismo de detección basado en el comportamiento del flujo.
- Machine learning no supervisado con ayuda de huellas estadísticas.
- Modelo basado en aprendizaje estadístico para la detección de anomalías.
- Redes neuronales con árboles de decisión.
- Sistema de detección autoadaptativo (basado en el aprendizaje profundo) utilizando el volumen de flujos de red del equipo de los usuarios de 5G.
- Modelo de juego evolutivo.
- Modelo de patrones potenciales con respecto a los recursos.
- Modelo estocástico para examinar varios factores que afectan el crecimiento.
- Detección jerárquica del tráfico de botnets utilizando modelos ocultos de Markov.
- Modelo de flujo de múltiples fases.
- AutoBotCatcher: basada en blockchain para Internet de las cosas.
- Máquinas de soporte vectorial.

Modelado a través de cadenas de Markov

Posibles ataques:

- Gusanos
- Poisoning
- Pollution

Propagación de malware en una red de computadoras o dispositivos móviles y actualmente es una de las principales amenazas a la seguridad de la información. La gran mayoría de los modelos propuestos se basan en ecuaciones diferenciales.

La actividad no autorizada de malware (carga útil) puede variar desde un simple borrado de archivos hasta la recuperación y uso posterior de información privada y / o confidencial.

Estos Malwars podrían clasificarse en: virus computacionales, troyanos, rootkits, spyware y otros como addwares, bombas lógicas, etc.

La gran mayoría de los modelos matemáticos se basan en el uso de ecuaciones diferenciales ordinarias o en ecuaciones diferenciales parciales, lo que significa que dichos modelos son de naturaleza continua. Por el contrario, si las herramientas matemáticas utilizadas son autómatas celulares, redes neuronales, máquinas de estados finitos, modelos basados en agentes, etc., obtendríamos modelos discretos. Intermedios entre estos se encuentran los modelos mixtos (aquellos en los que algunas variables son continuas y otras discretas) basados en ecuaciones de recurrencia, ecuaciones de retardo booleano, etc.

Los modelos matemáticos desarrollados para explorar la propagación de malware se basan en modelos diseñados para estudiar la diseminación de enfermedades infecciosas.

Los modelos epidemiológicos son compartimentales, que es decir, la población (a través de la cual se propaga la enfermedad infecciosa) se divide en diferentes tipos de comportamiento teniendo en cuenta las características de la enfermedad: susceptible, expuesta (con o sin síntomas), infecciosa, recuperada, en cuarentena, vacunada, aislada. , y así. Las denominaciones traducidas al caso del estudio de propagación de malware corresponden así a las siguientes: susceptibles (equipos que no han sido infectados por malware), expuestos (equipos que han sido infectados por malware pero aún no han sido activados), infecciosos (equipos en los que el código malicioso se encuentra en modo activo, teniendo así la capacidad de cumplir con su deber y propagarse a otros equipos de la red), en cuarentena (equipos detectados como infectados y retirados de la red para eliminar el virus), recuperados (equipos en los que se ha eliminado el malware), etc.

Los modelos deterministas se basan generalmente en ecuaciones diferenciales o ecuaciones en diferencias. Por otro lado, los modelos estocásticos se pueden clasificar en dos tipos

básicos: los basados en cadenas de Markov (modelos de cadena de Markov de tiempo discreto o modelos de cadena de Markov de tiempo continuo), donde la variable de estado es discreta, y los basados en ecuaciones diferenciales estocásticas. , donde tanto el tiempo como las variables de estado son continuas. Los modelos deterministas proporcionan buenos resultados cuando la población es muy grande: más de 10^5–10^6, mientras que los modelos estocásticos son más apropiados cuando se intenta simular la propagación de malware en redes de computadoras pequeñas, generalmente entre 10^2 y 10^5–10^6.

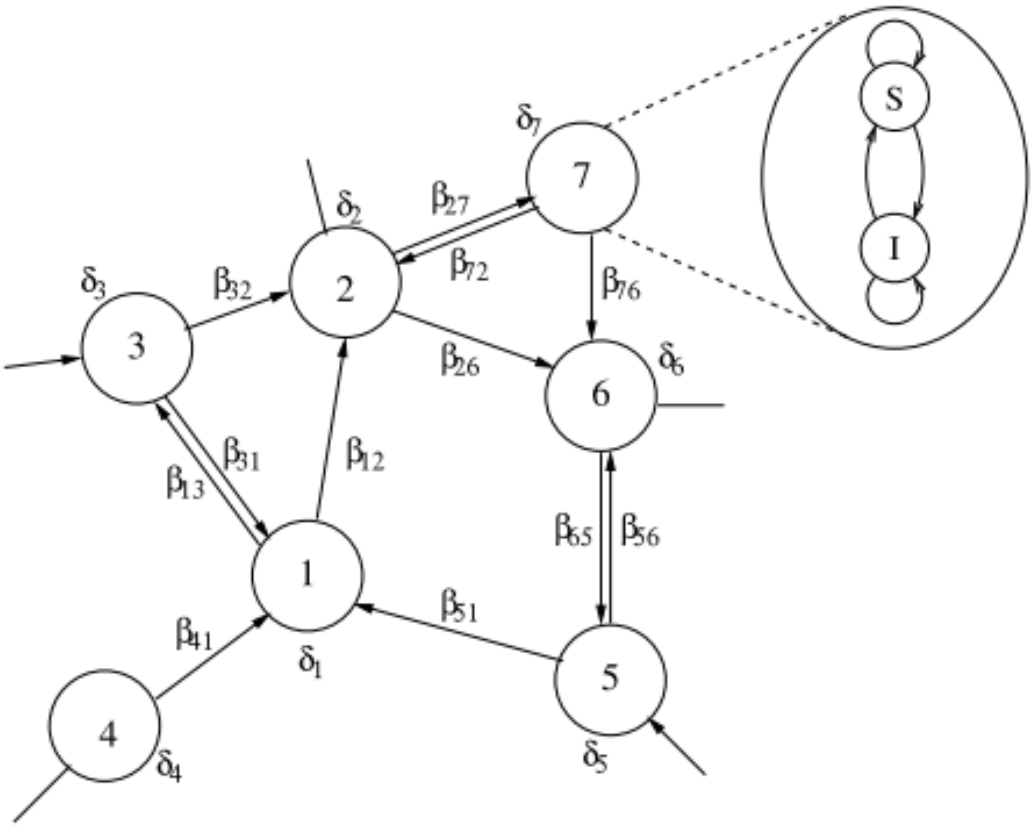

Figura 4: Ejemplo de una red considerando dos estados

En el caso de la simulación de la propagación de malware (es decir, estudio de la evolución de los distintos compartimentos en el tiempo), 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 o tasa de transmisión (que depende del contacto y la probabilidad de que un contacto conduzca a la transmisión), la tasa de recuperación (debido al efecto de las aplicaciones antivirus), el número de computadoras retiradas de la red, las probabilidades de pasar de un compartimento a otro, la probabilidad de adquisición de inmunidad (transitoria o indefinida), el período de latencia, el período de inmunidad, etc.

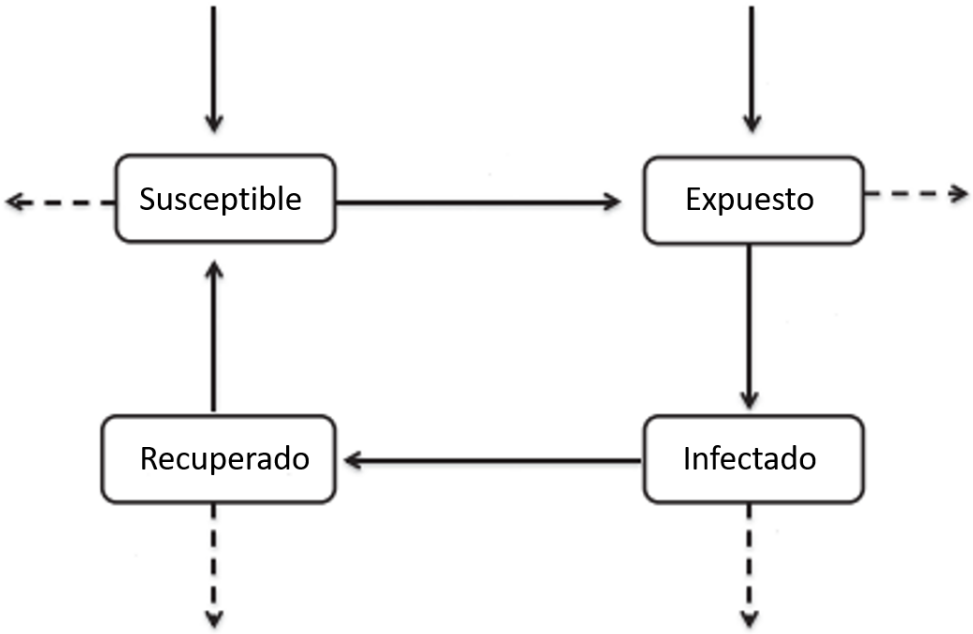

Figura 5: Diagrama del flujo entre los estados

Otro manera de propagación

Consideramos una red de N nodos donde la red está totalmente conectada, es decir, cualquier par de computadoras en funcionamiento pueden comunicarse. Cada computadora está equipada con un software antivirus que necesita actualizar regularmente las firmas antivirus para brindar la capacidad de eliminar virus informáticos. Suponemos que el momento de la actualización es aleatorio. Un nodo no funciona durante este tiempo. Cualquier computadora puede infectarse debido a las siguientes dos razones: ataques externos de virus (por ejemplo, visitar sitios tóxicos durante la navegación en la Web) y propagarse dentro de la red. Suponemos que los virus llegan a cada nodo de acuerdo con procesos de Poisson independientes con tasa , es decir, los intervalos entre ataques .exitosos"son variables aleatorias exponenciales independientes (es decir, rv) del parámetro . Clasificaremos los virus entrantes de la siguiente manera: (i) los virus de tipo I causan daños ocultos: acceso a información privada, robo de identidad, corrupción o eliminación de datos, adquisición de espacio en el disco duro o tiempo de la unidad central de procesamiento (CPU), registro de pulsaciones de teclas; (ii) los virus de tipo II causan fallas en el sistema; (iii) los virus de tipo III tienen las dos características (i) y (ii), por lo que son virus de tipo mixto. Denote por PI, PII, PIII porciones de virus entrantes de los tipos correspondientes: PI + PII + PIII = 1. Un nodo de trabajo infectado puede infectar cualquier nodo de trabajo saludable. Un nodo sano se infecta si entra en contacto con un nodo infectado. Suponemos que para cualquier par de computadoras, los intervalos entre comunicaciones son, es decir, r.v. del parámetro . El tiempo transcurrido hasta un fallo del sistema de un nodo infectado por los virus II o III es

aleatorio y se distribuye exponencialmente con una tasa .

Referencias

[1] Gaoxiang Chen y col. "An identity authentication scheme in wireless peer-to-peer network". En: *Int. Conf. Commun. Technol. Proceedings, ICCT* (2010), págs. 473-476. DOI: 10.1109/ICCT.2010.5688868.

[2] Ting Chen y col. *Active Worm Propagation Modeling in Unstructured P2P Networks*. 2009. ISBN: 9789525726077. URL: https://www.researchgate.net/publication/266268815.

[3] Jochen Dinger y Hannes Hartenstein. "Defending the sybil attack in P2P networks: Taxonomy, challenges, and a proposal for self-registration". En: *Proc. - First Int. Conf. Availability, Reliab. Secur. ARES 2006* 2006 (2006), págs. 756-763. DOI: 10.1109/ARES.2006.45.

[4] Muhammad Faheem Rasheed. *Modelling Virus Propagation in P2P Networks*. Inf. téc. 2012. URL: www.IJCSI.org.

[5] Sadek Ferdous, Farida Chowdhury y Md Moniruzzaman. "A Taxonomy of Attack Methods on Peer-to-Peer Network". En: *Proc. 1th Indian Conf. Comput. Intell. Inf. Secur.* 2007.April 2016 (2007), págs. 132-138.

[6] Gera Jaideep y Bhanu Prakash Battula. "Survey on the Present State-of-the-Art of P2P Networks, Their Security Issues and Counter Measures Article in". En: *Int. J. Appl. Eng. Res.* (2016). DOI: 10.37622/IJAER/11.1.2016.616-620. URL: https://www.researchgate.net/publication/298711927.

[7] Myung Suk Lee y Dae Jin Jang. "A survey of blockchain security issues". En: *JP J. Heat Mass Transf.* 2020.Special Issue 1 (2020), págs. 29-35. ISSN: 09735763. DOI: 10.17654/HMSI120029.

[8] Jian Liang, Naoum Naoumov y Keith W. Ross. "The index poisoning attack in P2P file sharing systems". En: *Proc. - IEEE INFOCOM* 00.c (2006). ISSN: 0743166X. DOI: 10.1109/INFOCOM.2006.232.

[9] Alexandra Mihaita y col. "Analysis of Security Approaches for Vehicular Ad-Hoc Networks". En: *Proc. - 2015 10th Int. Conf. P2P, Parallel, Grid, Cloud Internet Comput. 3PGCIC 2015* (2015), págs. 304-309. DOI: 10.1109/3PGCIC.2015.184.

[10] Zied Trifa y Maher Khemakhem. "Taxonomy of Structured P2P Overlay Networks Security Attacks". En: *World Acad. Sci. Eng. Technol.* 6.4 (2012), págs. 460-466.

[11] Chunling Wang y Jingyu Feng. "A study of mutual authentication for P2P trust management". En: *Proc. - 2010 6th Int. Conf. Intell. Inf. Hiding Multimed. Signal Process. IIHMSP 2010* (2010), págs. 474-477. DOI: 10.1109/IIHMSP.2010.121.

[12] Logan Washbourne. “A survey of P2P network security”. En: (2015), págs. 1-12. URL: http://arxiv.org/abs/1504.01358.