Advances in Artificial Intelligence

Grigori Sidorov (ed.)

Instituto Politécnico Nacional, Centro de Investigación en Computación
México 2016

Research in Computing Science

Series Editorial Board

Research in Computing Science es una publicación trimestral, de circulación internacional, editada por el Centro de Investigación en Computación del IPN, para dar a conocer los avances de investigación científica y desarrollo tecnológico de la comunidad científica internacional. **Volumen 113,** septiembre 2016. Tiraje: 500 ejemplares. *Certificado de Reserva de Derechos al Uso Exclusivo del Título* No. : 04-2005-121611550100-102, expedido por el Instituto Nacional de Derecho de Autor. *Certificado de Licitud de Título* No. 12897, *Certificado de licitud de Contenido* No. 10470, expedidos por la Comisión Calificadora de Publicaciones y Revistas Ilustradas. El contenido de los artículos es responsabilidad exclusiva de sus respectivos autores. Impreso en la Ciudad de México, en los Talleres Gráficos del IPN – Dirección de Publicaciones, Tres Guerras 27, Centro Histórico, México, D.F. Distribuida por el Centro de Investigación en Computación, Av. Juan de Dios Bátiz S/N, Esq. Av. Miguel Othón de Mendizábal, Col. Nueva Industrial Vallejo, C.P. 07738, México, D.F. Tel. 57 29 60 00, ext. 56571.

Editor responsable: *Grigori Sidorov*, *RFC SIGR651028L69*

Research in Computing Science is published by the Center for Computing Research of IPN. **Volume 113**, September 2016. Printing 500. The authors are responsible for the contents of their articles. Printed in Mexico City, in the IPN Graphic Workshop – Publication Office.

ISSN: 1870-4069

Instituto Politécnico Nacional (IPN)
Centro de Investigación en Computación (CIC)
Av. Juan de Dios Bátiz s/n esq. M. Othón de Mendizábal
Unidad Profesional "Adolfo López Mateos", Zacatenco
07738, México D.F., México

http://www.rcs.cic.ipn.mx
http://www.ipn.mx
http://www.cic.ipn.mx

Indexed in LATINDEX, DBLP and Periodica

Printing: 500

Printed in Mexico

Propagación de malware: propuesta de modelo para simulación y análisis

Luis Angel García Reyes[1], Asdrúbal López-Chau[1], Rafael Rojas Hernández[1], Pedro Guevara López[2]

[1] Universidad Autónoma del Estado de México, CU UAEM Zumpango, Zumpango, Estado de México, México

[2] Instituto Politécnico Nacional, Escuela Superior de Ingeniería Mecánica y Eléctrica Unidad Culhuacán, Ciudad de México, México

angel_garc@outlook.es, alchau@uaemex.mx, http://www.alchau.com

Resumen. La cantidad y diversidad de software malicioso (Malware) en la actualidad es enorme. Se espera que en un corto tiempo se incrementen todavía más las amenazas cibernéticas. Uno de los enfoques más utilizados para enfrentar este problema, es analizar la dinámica de propagación de Malware utilizando modelos matemáticos basados en sistemas de ecuaciones diferenciales propuestos en la década de los años 20. Una desventaja de ese enfoque es la dificultad que se presenta para relacionar el valor de los parámetros de las ecuaciones con aspectos específicos del mundo real. En este artículo, se presenta una propuesta para simular y analizar la propagación de Malware considerando elementos que se presentan cotidianamente en la realidad. Se propone un modelo en el que se introducen dos conceptos nuevos, el primero es remarcar la diferencia entre individuos y dispositivos; el segundo es realizar la distinción entre propietarios y usuarios de dispositivos. Estos elementos son introducidos como parámetros del modelo para analizar la evolución de la propagación. El modelo presentado se implementó como una plataforma funcional, que se utilizó para realizar simulaciones con 1,000 dispositivos. De acuerdo a los resultados de los experimentos realizados, se encuentra evidencia del efecto de los conceptos introducidos sobre la dinámica de propagación de Malware.

Palabras clave: Malware, propagación, plataforma de simulación, virus.

Malware Propagation: Proposal of the Model for Simulation and Analysis

Abstract. The amount and diversity of malicious software (Malware) today is huge. It is expected a further increase of cyberthreat in a short

time. One of the most commonly used approaches to address this problem is to analyze the dynamics of Malware propagation using mathematical models based on systems of differential equations. These were proposed in the decade of the 20s. One disadvantage of this approach is the difficulty presented to relate the value of the parameters of the equations with specific aspects of the real-world. In this paper, a proposal is presented to simulate and analyze the spread of Malware considering elements that occur daily in reality. A model in which two new concepts are introduced is proposed, the first concept is to emphasize the difference between individuals and devices; the second one is to make the distinction between owners and users of devices. These elements are introduced as parameters of the model to analyze the evolution of the spread. The model was implemented as a functional platform, which was used for simulations with 1,000 devices. According to the results of experiments, it is evidence of the effect of the concepts introduced on the dynamics of spreading Malware.

Keywords: Malware, propagation, simulation platform, virus.

1. Introducción

La seguridad de los sistemas informáticos es considerada como un aspecto vital tanto por empresas como por usuarios finales. Uno de los elementos más importantes que ponen en peligro la seguridad de este tipo de sistemas es la presencia de programas malignos o software malicioso (Malware) en el sistema operativo (SO) de los dispositivos.

De acuerdo a los últimos reportes de algunas de las principales empresas dedicadas a la seguridad informática [10], [11], [5], la tendencia en los próximos meses es que aumente tanto el número como las variantes de las amenazas.

Con el objetivo de enfrentar al Malware, empresas e investigadores han invertido esfuerzos considerables para tratar de entenderlo desde diversos ángulos. Uno de los aspectos que ha atraído la atención de la comunidad científica en los últimos años, es la creación de modelos de la propagación del software malintencionado. Esto debido a que con ellos se pueden realizar estimaciones sobre la rapidez con la que un Malware podría infectar a todos los dispositivos en una red, o incluso a una cantidad considerable de dispositivos del mundo entero, lo que permite tomar medidas antes de que ocurran daños significativos en las organizaciones.

La mayoría de los modelos de propagación de Malware propuestos hasta la fecha, están basados en los modelos deterministas epidemiológicos tipo SIR (Susceptible, Infectado y Recuperado), y una plétora de variantes. Estos modelos usan ecuaciones diferenciales de primer orden con coeficientes constantes. La principal ventaja de estos modelos es su simplicidad. Sin embargo, uno de los problemas es que para la mayoría de las aplicaciones, no resulta sencillo relacionar el valor de los coeficientes con elementos del mundo real.

En este artículo, presentamos una plataforma para estudiar la propagación de Malware implementado como una aplicación de escritorio Java (Para obtener el código fuente ver [4]). La plataforma presentada contiene una serie de parámetros simples de entender, que están directamente relacionados con elementos reales, tal como la cantidad de usuarios, cantidad de dispositivos, número de dispositivos infectados al inicio de la simulación, y otros. La aplicación permite simular paso a paso la dinámica de la infección, y presentar los resultados de manera tabular y gráfica.

El resto del artículo se encuentra organizado en 6 secciones. La Sección 2 presenta la definición Malware, así como los principales tipos y formas de propagación más conocidas. Una revisión de los trabajos relacionados se encuentra en la sección 3. El modelo propuesto y su implementación son presentados en la sección 4. Los resultados de las simulaciones y una discusión de los mismos están presentes en la sección 5. Las conclusiones de la investigación y trabajos futuros pueden leerse en la sección 6.

2. Malware

El término Malware proviene del inglés "malicious software", que en español significa código malicioso [3], [6]. Técnicamente, Malware se refiere a programas que se instalan en los SO de los equipos con desconocimiento de los usuarios. Estos programas esperan silenciosamente su ejecución con la intención de causar daños con acciones inadecuadas u objetivos maliciosos. Por lo tanto, hablar de software malicioso involucra amenazas constantes en los SO.

Existen diferentes tipos de software malicioso. Un virus informático infecta los dispositivos viajando de manera autónoma entre ellos, normalmente, esperando a ser detonado por un usuario final. Un gusano (Worm) es programado también para viajar entre los dispositivos, pero este tipo de software sólo se instala una vez dentro del sistema, y posteriormente busca otro dispositivo para su infección. Algunos gusanos requieren de la interacción con usuarios, pero también existen algunos de ellos que logran infectar sin la necesidad de dicha interacción. Los troyanos (Trojans), por otro lado, hacen honor a la leyenda mítica griega "Caballo de Troya", debido a que el software no aparenta ser mal intencionado, sino todo lo contrario, parece ser un software útil para el usuario. Los troyanos también pueden ser instalados sin la necesidad de ser descubiertos o detonados por un usuario, permitiéndose así el acceso al sistema sin aviso alguno. Estos son mejor conocidos como troyanos de puerta trasera (Trojans Backdoors). A diferencia de los virus y los gusanos, los troyanos dependen del acceso a Internet. Otro tipo de Malware que se ha popularizado en los últimos años, son los llamados Spyware del tipo de infiltración silenciosa. Estos pretenden la obtención de información de los usuarios. Entre los datos más importantes que puede llegar a sustraer esta amenaza, se encuentran las contraseñas y números de tarjetas de crédito.

Un tipo de amenaza llamado *phishing* ha tenido una gran actividad recientemente. La finalidad del phishing es sustraer información de usuarios

usando una estrategia diferente a los troyanos. Se presenta a los usuarios una interfaz (página Web) de alguna entidad de confianza, por ejemplo banco u otra organización empresarial. El usuario puede ser engañado y proporcionar datos tales como su nombre de usuario, contraseña o número generado por dispositivo electrónico "token". La forma de hacer llegar a los usuarios los enlaces es a través de correo electrónicos o mensajes [10].

Actualmente, diversos tipos de Malware son capaces de burlar a los sistemas de prevención implementados en diversos SO, esto debido principalmente a la falta de mantenimiento o de actualización de los equipos con acceso a Internet considerando aspectos cómo la falta de cultura informática por parte de los usuarios, lo que les impide tomar las medidas necesarias contra este tipo de software.

Hay diferentes maneras de infectar los dispositivos con Malware. Una cantidad importante de ellas se relaciona con las actividades que se realizan cotidianamente, como la recepción de correo electrónico y mensajes con archivos adjuntos contaminados. Otra forma es visitando páginas Web aparentemente inofensivas, pero que tienen vínculos a descargas y/o instalación Malware. El compartir archivos en red o a través de algún medio extraíble como lo son CDs, USB, HDD portable, DVD entre otros, es también otra manera de infectar equipos con Malware [1].

Por otro lado, las técnicas de propagación de estos programas maliciosos los hacen capaces de multiplicarse bajo la intrusión a través de la red e infectar a un sinnúmero de sistemas [3], [6].

3. Trabajos relacionados

Uno de los enfoques más ampliamente utilizados para modelar la propagación de Malware es la aplicación del modelo epidemiológico SIR (o simplemente SIR de aquí en adelante) desarrollado por Kermack y McKendrick en 1927 [7] para estudiar la propagación de enfermedades en cortos periodos de tiempo. SIR permite estimar la cantidad de individuos de una población que son susceptibles de contraer una enfermedad, así como la cantidad de individuos de la población que han sido infectados por esa misma enfermedad y el número de individuos que se han recuperado.

Las ecuaciones diferenciales ordinarias que modelan la dinámica de infección son las siguientes [8]:

$$\frac{dS(t)}{dt} = -\beta I(t)S(t) \qquad \frac{dI(t)}{dt} = \beta I(t)S(t) - \alpha I(t),$$
$$\frac{dR(t)}{dt} = \alpha I(t),$$

cuya solución es:

$$S(t) = S(0)e^{\frac{-\beta}{\alpha}R},$$
$$I_{max} = -\frac{\alpha}{\beta} + \frac{\alpha}{\beta}\ln\left(\frac{\alpha}{\beta}\right) + S(0) + I(0) - \frac{\alpha}{\beta}\ln S(0),$$

donde:

- Se asume que una cantidad de individuos susceptibles S(t), se encuentra en contacto con individuos ya infectados I(t), a través de una mezcla homogénea. Además, cada individuo es idéntico al resto.
- La cantidad de individuos que se recuperan (y que no pueden volver a infectarse) se representa con R(t).
- El tamaño N de la población es constante, lo que implica que N=S(t)+I(t)+R(t).
- El número de individuos infectados que contagia a otros susceptibles a una tasa de infección β (denominada *transmission rate constant*). Cada individuo infectado es infeccioso.
- La tasa de recuperación de los individuos es α. Si no se considera la recuperación, entonces este parámetro es igual a cero.
- I_{max} es el máximo número de individuos infectados en la epidemia.

Desde la aparición de SIR, se han desarrollado variantes interesantes aplicadas a diversas topologías de redes de dispositivos electrónicos.

En [9], se muestra un estudio detallado de la aplicación de un modelo analítico para el proceso SIS (por las siglas en inglés *susceptible infected susceptible*). En este modelo, se usa el concepto de çontactos", que son usados para propagar un virus informático o biológico. La probabilidad de que un individuo se infecte está en función del promedio de los vecinos infectados. Aunque analíticamente este modelo es atractivo, la dificultad más notable es la complejidad para relacionar directamente sus parámetros con elementos del mundo real.

Un enfoque diferente para estudiar la propagación de Malware, es emplear una simulación por computadora. En [2] se propone EpiNet, un framework para simular propagación de gusanos informáticos en redes masivas Bluetooth de smartphones. Tanto el modelo propuesto, como las conclusiones presentadas en [2], son interesantes e importantes para entender el proceso de propagación de gusanos informáticos. Sin embargo, entre las desventajas más importantes de este framework se pueden mencionar las siguientes: 1) se considera que dos dispositivos conectan si están lo suficientemente cercanos físicamente (10 m, para dispositivos BT clase II). 2) Además, la topología de la red toma un rol importante en EpiNet. Ambas consideraciones no son adecuadas actualmente, debido a restricciones tales como el ahorro de energía (Bluetooth apagado), o la necesidad de que los usuarios autoricen las conexiones a redes.

En la siguiente sección, se presenta el modelo propuesto en este artículo para analizar la propagación de Malware.

4. Modelo propuesto

En el diseño del modelo presentado, se tomaron en cuenta algunos aspectos del mundo real que se consideran importantes, y que hasta donde sabemos, no se encuentran presentes en otros artículos publicados anteriormente en la literatura especializada.

El primer aspecto es la diferencia entre dispositivo e individuo. Los dispositivos pueden infectarse, mientras que los individuos no. Por lo tanto, a diferencia de otros modelos, en el nuestro, un mismo individuo puede a veces contagiar a otro dispositivo, dependiendo si usa un equipo infectado o no para enviar mensajes.

El segundo aspecto es la introducción del concepto de usuario y propietario. Un usuario puede usar equipos diferentes para enviar o recibir mensajes, mientras que un propietario siempre usa el mismo dispositivo. Estos conceptos son importantes, ya que permiten capturar la realidad que ocurre en escuelas, cafés Internet o cualquier otro espacio donde varios usuarios comparten equipos.

4.1. Elementos del modelo propuesto

Los principales elementos del modelo propuesto son los siguientes:

1. *Dispositivo.* Se refiere a una computadora, teléfono inteligente o cualquier otro equipo electrónico capaz de enviar y recibir mensajes de diversos tipos, y que pueda contagiarse de Malware.
2. *Mensaje.* Los mensajes pueden ser correo electrónico, enlaces, texto o multimedia, enviados o recibidos por aplicaciones que se ejecutan en dispositivos electrónicos. La infección se da al leer desde un dispositivo susceptible, un mensaje que ha sido enviado desde un dispositivo infectado.
3. *Usuario.* Son individuos que usan dispositivos electrónicos para recepción y envío de mensajes. En nuestro modelo, a diferencia de otros, los individuos pueden usar varios dispositivos infectados para propagar Malware.
4. *Propietario.* Son individuos que siempre usan el mismo dispositivo para la comunicación con otros individuos.
5. *Lista de contactos.* Cada individuo tiene una lista de contactos a los cuales envía mensajes. Este concepto es semejante al usado en [9].

El modelo del mecanismo de infección se propone simple, pero lo suficientemente flexible para poder adaptarse a mecanismos de infecciones más

avanzados, tales como robo de lista de contactos y envío automático de mensajes. Algoritmo 1 muestra el proceso general de infección implementado.

Algoritmo 1: Infección de dispositivos con Malware

Input: ;
M: Mensaje recibido;
U_i: individuo i-ésimo;
D_j: Dispositivo actual usado para leer M
Output: Nada

```
1 Individuo U_i lee mensaje recibido M desde dispositivo D_j
2 if M contiene Malware adjunto then
3     D_j es infectado
4     D_i adjuntará Malware la siguiente vez que sea usado para enviar
      mensaje.
```

La simulación de la propagación de Malware sigue el proceso mostrado en Algoritmo 2.

Algoritmo 2: Proceso general de la simulación

Input: ;
N: Número de individuos;
D: Número de dispositivos;
P: Número de propietarios;
TotalPasos: Número de pasos en la simulación;
S: Semilla del generador de números pseudoaleratorios;
C_{max}, C_{min}: Número de máximo y mínimo de contactos;
T_{max}: Número de contactos a los que se le envía mensaje
Output: Total dispositivos infectados

```
1 Crear lista de contactos aleatoriamente para cada individuo.
2 Asignar computadoras a usuarios
3 Asignar computadoras a propietarios
4 for paso=1: TotalPasos do
5     foreach individuo con equipo asignado do
6         Leer mensajes recibidos
7         Enviar un mensaje a un máximo de T_max individuos de la lista de
          contactos, estos son elegidos pseudo-aleatoriamente.
8     Re asignar computadoras a usuarios (propietarios se mantienen en el mismo
      dispositivo)
9 return Número de dispositivos infectados
```

Las principales características del modelo propuesto son las siguientes:

- Dispositivos vs individuos. A diferencia de los modelos epidemiológicos como SIR, donde un individuo infectado no puede volver a infectarse, en el modelo propuesto un individuo puede contribuir a infectar más de un dispositivo. Además, los individuos no se contagian.

- Independencia de la topología de red. Esto se consideró así, ya que actualmente, no es necesario estar conectado a una misma red para envío y recepción de mensajes.
- Mensaje como medio de infección. Estos mensajes pueden ser enlaces o Malware.
- Posibilidad de rotación entre dispositivos e individuos. Un mismo dispositivo puede ser usado por varios individuos (usuarios), o siempre por el mismo (propietario). La finalidad de esto es capturar la realidad de que los equipos se pueden compartir.

En la siguiente subsección, se presentan algunos detalles de la implementación del modelo desarrollado.

4.2. Plataforma desarrollada

La plataforma desarrollada fue programada en lenguaje Java y su arquitectura general se muestra en la Figura(1).

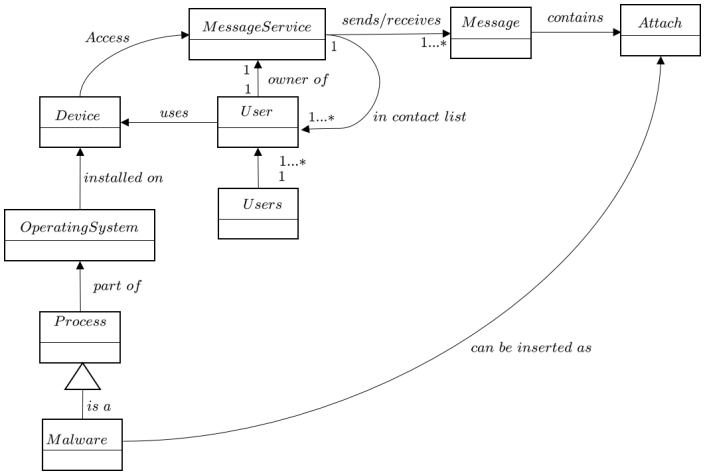

Fig. 1. Arquitectura general propuesta de la plataforma para simulación de propagación de Malware.

En la arquitectura propuesta se puede observar que cada *Individuo* no se contagia, sino un *Dispositivo* que es usado para leer *Mensajes*. El módulo Malware está relacionado con el módulo Dispositivo (Device en la Figura 1) a través del Sistema Operativo. Un dispositivo infecta a otro cuando le envía un anexo (Malware) en un mensaje, esto sin conocimiento del usuario del dispositivo infectado.

Aunque no es parte fundamental de la arquitectura general, en la implementación también se encuentran presentes otros elementos que permiten monitorizar el estado de los dispositivos, la asignación de dispositivos a usuarios y la cantidad de dispositivos infectados, entre otras variables.

5. Experimentos y resultados

En los modelos epidemiológicos usados para simular la propagación de Malware, puede modificarse el valor de unos cuantos parámetros, y observar la solución del sistema de ecuaciones diferenciales, presentando únicamente la cantidad de individuos infectados, susceptibles o recuperados por unidad de tiempo. Aunque esto es útil debido a su sencillez, no se permite explorar en detalle varios aspectos del mundo real que intervienen, como por ejemplo, cómo afecta a la velocidad de propagación la cantidad de mensajes recibidos o enviados, la relación entre la cantidad de usuarios en la lista de contactos y la tasa de propagación, etc.

En esta sección, se realiza una exploración de varios factores del mundo real que son capturados por el modelo propuesto, y se presentan las gráficas que muestran la evolución de la propagación. Se eligieron las siguientes variables para los experimentos:

1. Número de equipos infectados inicialmente. Esta simulación es común encontrarla en publicaciones similares, debido a que permite conocer en qué tiempo se espera tener a toda la población infectada, en función de los dispositivos inicialmente infectados de Malware.
2. Número de propietarios y número de dispositivos infectados inicialmente. El concepto de propietario y usuario es un aspecto novedoso en nuestro modelo, por lo que esta simulación no ha sido presentada anteriormente.
3. Tamaño de la lista de contactos. Este parámetro tiene que ver con la cantidad de usuarios que tienen contacto entre sí, y que por ende pueden contagiarse.

En experimentos preliminares, se encontró que la evolución de la propagación de Malware tiene una tendencia similar con diferentes números de dispositivos y de usuarios. Este comportamiento se encuentra presente también los modelos basados en ecuaciones diferenciales. Con la intensión de que en las gráficas presentadas se pueda apreciar mejor el comportamiento de la propagación de Malware, se decidió que el número de dispositivos y de usuarios fuera 1,000. Además, en cada experimento se realizaron 100 simulaciones, graficando el promedio de la cantidad de dispositivos infectados en cada unidad tiempo. Un número mayor de simulaciones, produce resultados con variación mínima en los resultados (menor al 0.05 %).

Usando los parámetros mencionados anteriormente, se encontró que la totalidad de equipos son infectados en menos de 50 pasos o unidades de tiempo, (parámetro TotalPasos en Algoritmo 2). En cada paso, el monitor implementado realizó un conteo de los equipos infectados. El generador de números pseudo-aleatorios de Java, usado para elegir individuos en la lista de

Cuadro 1. Parámetros usados en la simulación I y II

Parámetro	Sim I	Sim II
Total individuos (N)	1,000	1,000
Total dispositivos (D)	1,000	1,000
Propietarios (P)	15	5
Mínimo de contactos (C_{min})	5	5
Máximo de contactos (C_{max})	15	15
Contactos a los que se envía mensaje (T_{max})	1	1

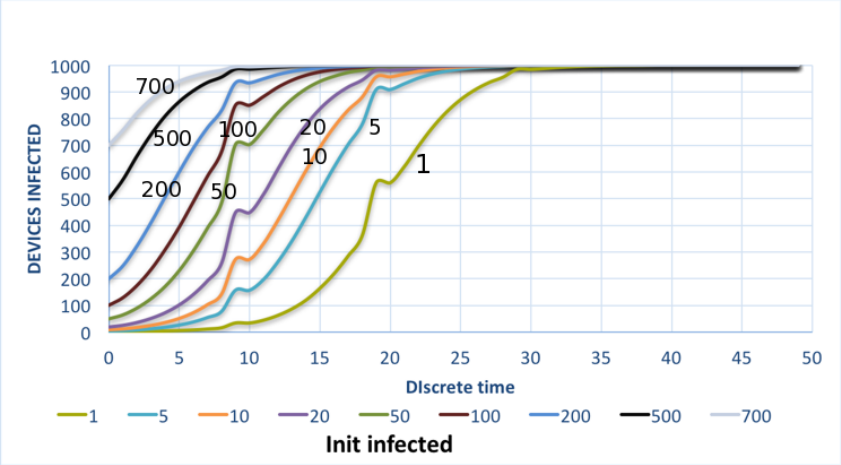

Fig. 2. Evolución de la propagación de Malware, simulación I.

contactos, toma como semilla el tiempo en que comienza un proceso de infección, usando el método estático *nanoTime()* de la clase System de Java.

Simulación I, número de dispositivos infectados inicialmente En este experimento, se varía la cantidad inicial de dispositivos que han sido infectados por Malware, mientras que los parámetros mostrados en la Tabla 1 se mantienen fijos.

La Figura 2 muestra la evolución de la propagación de Malware para esta simulación. Como es de esperarse, entre mayor sea la cantidad de dispositivos infectados inicialmente, el tiempo en que la totalidad de equipos se infecta es menor.

Es importante notar que en la Figura 2 parecería que hay una disminución en la cantidad de dispositivos infectados, sin embargo, esto no sucede en la versión actual nuestro modelo, ya que no se encuentra incorporado un mecanismo

de recuperación en el SO de los dispositivos simulados. Al analizar los datos, se encontró que esta aparente disminución se debe a un redondeo que hace la herramienta usada para graficar los datos.

Simulación II, número de propietarios y usuarios En el segundo experimento, se exploró cómo influye en la evolución de propagación de Malware, la cantidad de usuarios (propietarios) que siempre usan el mismo dispositivo para enviar o recibir mensajes . La cantidad de dispositivos infectados también se varió, con el objetivo de investigar si hay alguna efecto significativo en el comportamiento de la propagación. Los parámetros utilizados son los mostrados en la Tabla 1.

En la figura 3 puede observarse la cantidad de dispositivos infectados con respecto al tiempo. El parámetro P tiene un efecto interesante; la evolución de propagación de Malware pierde sensibilidad con respecto a la cantidad de equipos infectados inicialmente. Es decir, aún cuando la cantidad de dispositivos inicialmente infectados con Malware aumenta, el cambio principal en curva de crecimiento se concentra entre 10 y 15 unidades de tiempo.

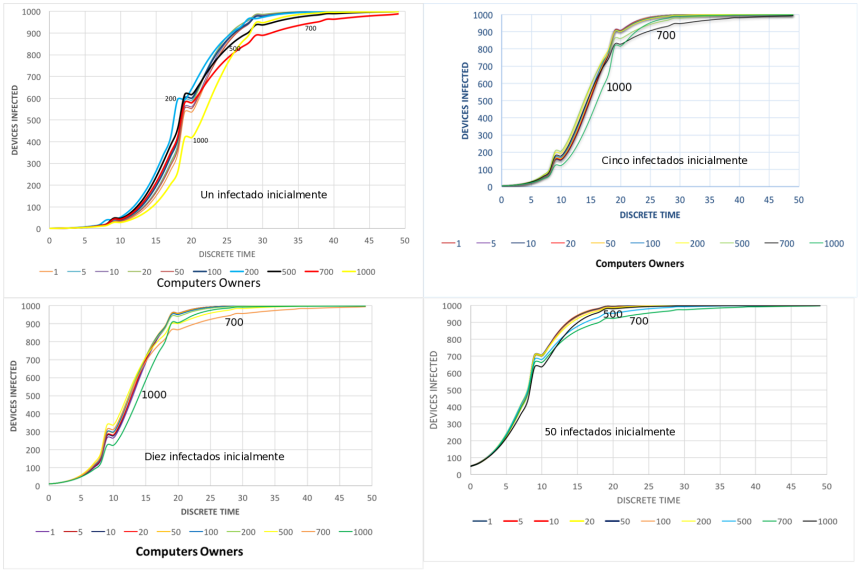

Fig. 3. Evolución de la propagación de Malware, simulación II.

Simulación III, tamaño de lista de contactos En el tercer experimento, se estudia el efecto que tiene el tamaño de la lista de contactos sobre la evolución de

la propagación de Malware. Los valores de los parámetros usados son similares a los de la simulación II, sólo se varían los valores del tamaño de la lista de contactos y el número de dispositivos infectados inicialmente . En la Figura 4 pueden observarse las gráficas resultantes.

En esta simulación, se observa que el número de dispositivos infectados al inicio, sí afecta notablemente el comportamiento de la propagación.

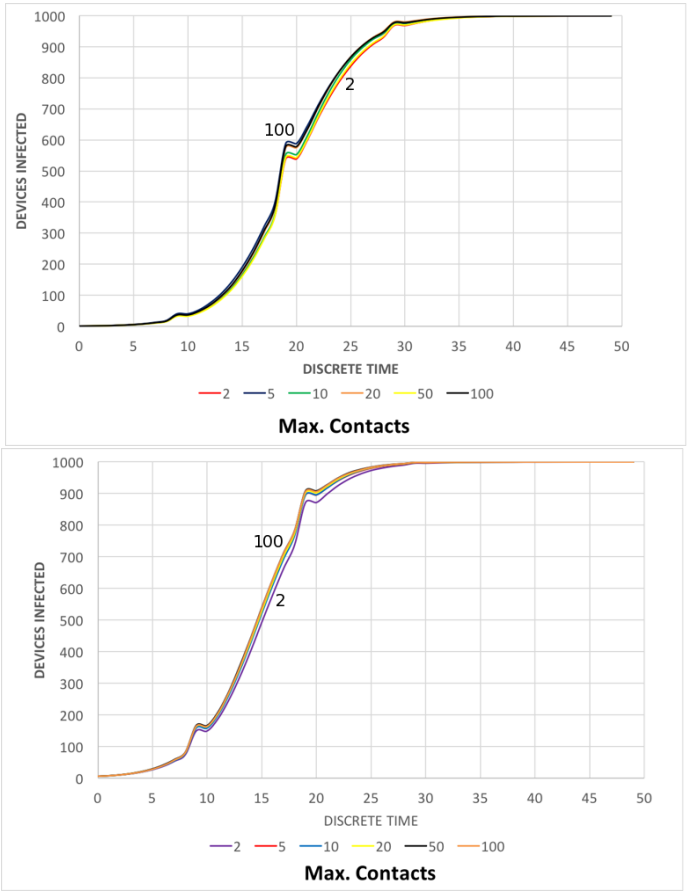

Fig. 4. Evolución de la propagación de Malware, simulación III.

6. Conclusiones y trabajo futuro

El estudio sobre propagación de Malware es de vital importancia actualmente, ya que el número de amenazas cibernéticas está en constante crecimiento. Uno de los enfoques para analizar la propagación de Malware, es utilizar representaciones matemáticas basados en el modelo SIR. En esta investigación, se propone un enfoque diferente para realizar este análisis. Se presenta el diseño y la implementación de una plataforma software para la simulación y el análisis de la propagación de Malware. El código fuente escrito en lenguaje Java puede ser descargado libremente usando la dirección mostrada en [4]. Esto con la finalidad de que otros investigadores puedan reutilizarlo.

La plataforma desarrollada está basada en un modelo que representa una abstracción de la realidad, en la que intervienen diversos elementos. Se presentan también dos aspectos novedosos; el primer aspecto que se propone es diferenciar entre usuario y dispositivo. De esta forma, los elementos que se infectan son los dispositivos y no los individuos, como ocurre en otros modelos. El segundo aspecto innovador es la introducción de los conceptos de usuario y propietario. Estos fueron considerados debido a que es común que un conjunto de equipos puede ser usado por varios individuos en diferentes tiempos, tal como ocurre en escuelas o cafés Internet.

Usando la plataforma propuesta, se puede analizar la dinámica de infección de una población con diferentes parámetros. En los experimentos presentados, se encontraron algunos efectos que tienen los parámetros en la evolución de la propagación de Malware.

Entre los trabajos futuros para esta investigación, se encuentran los siguientes: 1) realizar una comparativa de los resultados obtenidos con las respuestas que proporcionan los modelos epidemiológicos. Esto con el objetivo de encontrar la relación que existe entre los parámetros de las ecuaciones diferenciales, y aspectos del mundo real considerados en nuestra propuesta; 2) habilitar la plataforma para simulaciones de propagación de Malware a gran escala. Es decir, proveer la capacidad para simular millones de dispositivos e individuos; 3) implementar simulaciones de elementos de protección en los dispositivos, tales como programas anti Malware o anti SPAM y 4) Realizar más simulaciones para explorar la forma en que cada parámetro afecta a los otros.

Referencias

1. of Cambridge, U.: Computer viruses and other malware: what you need to know. http://www.ucs.cam.ac.uk/security/malware (2015)
2. Channakeshava, K., Chafekar, D., Bisset, K., Kumar, V.S.A., Marathe, M.: Epinet: A simulation framework to study the spread of malware in wireless networks. In: Proceedings of the 2Nd International Conference on Simulation Tools and Techniques. pp. 6:1–6:10. Simutools '09, ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), ICST, Brussels, Belgium, Belgium (2009), `http://dx.doi.org/10.4108/ICST.SIMUTOOLS2009.5652`

3. Fuentes, L.F.: Malware, una amenaza de internet. http://www.revista.unam.mx/vol.9/num4/art22/art22.pdf (Apr 2008)
4. García Reyes, L.A., López-Chau, A., Hernández, R., Guevara López, P.: Código fuente: Propagación de malware, propuesta de modelo para simulación y análisis. https://onedrive.live.com/redir?resid=993677954F59B48C!105155 &authkey=!AOov_R3KxgRp1yM&ithint=folder % 2czip (May 2016)
5. Garnaeva, M., Wie, J.v.d., Makrushin, D., Ivanov, A., Namestnikov, Y.: Kaspersky security bulletin 2015. overall statistics for 2015. https://securelist.com/analysis/kaspersky-security-bulletin/73038/kaspersky-security-bulletin-2015-overall-statistics-for-2015/ (December 2015)
6. Jiménez Rojas, J.R., Soto Astorga, R.d.P.: Qué es malware? http://www.seguridad.unam.mx/usuario-casero/eduteca/main.dsc?id=193 (2009)
7. Kermack, W., McKendrick, A.: A contribution to the mathematical theory of epidemics. Proc. R. Soc. Lond. A 115 pp. 700,721 (1927)
8. Martcheva, M.: An introduction to mathematical epidemiology. Texts in applied mathematics, Springer, Boston, MA (2015), http://cds.cern.ch/record/2112928
9. Mieghem, P.V.: The viral conductance of a network. Computer Communications 35(12), 1494 – 1506 (2012), http://www.sciencedirect.com/science/article/pii/S0140366412001405
10. Security, P.: Pandalabs detected more than 21 million new threats during the second quarter of 2015, an increase of 432014. http://www.pandasecurity.com/mediacenter/news/pandalabs-detected-more-than-21-million-new-threats/ (September 2015)
11. Symantec: 2015 internet security threat report, volume 20. http://www.symantec.com/security_response/publications/threatreport.jsp (2015)