UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO
POSGRADO EN CIENCIA E INGENIERÍA DE LA COMPUTACIÓN
INSTITUTO DE INVESTIGACIONES EN MATEMÁTICAS APLICADAS Y EN SISTEMAS
REDES Y SEGURIDAD EN CÓMPUTO

MODELADO DE PROPAGACIÓN DE GUSANOS EN TELÉFONOS INTELIGENTES A TRAVÉS DE BLUETOOTH USANDO AUTÓMATAS CELULARES

T E S I S

QUE PARA OPTAR POR EL GRADO DE
MAESTRO EN CIENCIA E INGENIERÍA DE LA COMPUTACIÓN

PRESENTA:
GABRIEL GONZÁLEZ GARCÍA

Tutor:
Dra. María Elena Lárraga Ramírez
Instituto de Ingeniería

Ciudad Universitaria, Cd. Mx. enero 2017

Agradecimientos

A mis sinodales, los doctores Luis Álvarez Icaza, Javier Gómez Castellanos, Carlos Gershenson García y al ingeniero Mario Rodríguez Manzanera por haber compartido su valiosa experiencia conmigo y haber enriquecido este trabajo.

A mi tutora, la Dra. María Elena Lárraga Ramírez por su esfuerzo, tiempo y dedicación puestos en el desarrollo de este trabajo, así como los consejos que me dio para enriquecerlo y su interés por difundirlo.

Agradezco a las instituciones que hicieron posible la realización de esta tesis: al Posgrado en Ciencia e Ingeniería de la Computación de la Universidad Nacional Autónoma de México, por darme la oportunidad de estudiar una maestría de excelencia; al Consejo Nacional de Ciencia y Tecnología (CONACyT) la beca que se me otorgó para la realización de mis estudios de maestría y finalmente al proyecto PAPIIT_DGAPA IN112716 por el apoyo otorgado para la realización de este trabajo de tesis y su difusión.

Resumen

En los últimos años, el uso de los teléfonos inteligentes (smartphones) se incrementa de manera continua debido a la extensa variedad de aplicaciones que se pueden instalar para su uso en el trabajo, estudio o recreación. La navegación e intercambio de información en internet se ve beneficiada por la mejora de las redes inalámbricas (Wi-Fi), facilitando el envío y recepción de correos electrónicos en cualquier momento, así como la realización de diversas transacciones en línea. Sin embargo, ello también ha motivado la proliferación de software malicioso (malware) diseñado específicamente para smartphones. Ante esta situación, el desarrollo de modelos para entender, analizar y estudiar la propagación de un programa de cómputo nocivo en teléfonos inteligentes con la finalidad de predecir y prevenir ha llegado a ser fundamental.

En este trabajo se desarrolló un nuevo modelo basado en autómatas celulares (AC) y modelos matemáticos epidemiológicos para caracterizar la dinámica de propagación de malware tipo gusano sobre Bluetooth. De tal manera que el modelo toma en cuenta las interacciones locales entre teléfonos inteligentes y es capaz de simular la evolución individual de cada dispositivo en el tiempo y el espacio. Los objetivos se orientaron a proponer un modelo diferente a los modelos de AC existentes, que tome en cuenta aspectos de seguridad y movilidad de los dispositivos que a la fecha no se han considerado con otros modelos existentes, para analizar y entender la propagación del malware bajo diferentes condiciones y medidas de control.

Resultados de simulación indican que el modelo captura la de dinámica de la propagación del gusano sobre Bluetooth y puede ser adecuado para evaluación y predicción. El costo computacional del modelo propuesto es bajo y preserva simplicidad, lo que lo hace adecuado para simular áreas geográficas grandes.

Abstract

In recent years, the use of smartphones increases continuously due to the wide variety of applications that can be installed for use at work, study or recreation. Navigation and exchange of information on the Internet is benefiting from improving (Wi-Fi) wireless networks, facilitating the sending and receiving emails at any time, as well as performing various online transactions. However, this has also led to the proliferation of malicious software (malware) designed specifically for smartphones. In this situation, the development of models to understand, analyze and study the spread of harmful computer program on smartphones in order to predict and prevent has become essential.

In this work, I developed a new model based on Cellular Automata (CA) and epidemiological mathematical models to characterize the dynamics of spread of malware of worm type on Bluetooth antennas. This model takes into account local interactions between smartphones and is able to simulate the individual performance of each device in time and space. The objectives aimed to propose a different AC model from existing ones, which takes into account safety aspects and mobility devices to date have not been considered with other existing models to analyze and understand the spread of malware under different conditions and control measures.

Simulation results indicate that the model captures the dynamics of the spread of the worm on Bluetooth and may be suitable for assessment and prediction. The computational cost of the proposed model is low and preserves simplicity, which makes it suitable for simulating large geographic areas.

Índice de Contenido

Índice de Figuras

Índice de Tablas

Introducción

Hoy en día, Internet es el mayor sistema de ingeniería jamás creado, con cientos de millones de computadoras conectadas mediante diversos enlaces de comunicación; con miles de millones de usuarios que se conectan empleando computadoras portátiles (laptops), tabletas y teléfonos inteligentes; y con una serie de diversos dispositivos conectados a Internet tales como sensores, cámaras web, consolas de video juegos, marcos fotográficos e incluso, aparatos electrodomésticos. Podemos definir el Internet como una red de computadoras que interconectan millones de dispositivos de cómputo a lo largo de todo el mundo [1]. No hace mucho tiempo, estos dispositivos eran en su mayoría PCs tradicionales de escritorio, estaciones de trabajo Unix o Linux, y los llamados servidores que almacenaban y transmitían información como páginas Web y correo electrónico. Sin embargo, dispositivos finales no tradicionales de Internet como laptops, automóviles, sensores ambientales, sistemas de seguridad, teléfonos inteligentes, entre otros, se conectan a Internet con el propósito de intercambiar información de cualquier tipo. Así, cada día vemos más dispositivos de este tipo como herramienta de venta, catálogo de producto, herramienta de gestión de siniestros o contratos, o simplemente como instrumento de uso recreativo. Este hecho aunado al consumismo por estos dispositivos y fenómenos como el BYOD (Bring Your Own Device) ha alterado las necesidades de las empresas, tanto a nivel del área de tecnología de información como de los usuarios finales.

Particularmente, la proliferación de teléfonos inteligentes se ha incrementado a un ritmo vertiginoso; de acuerdo al Telegraph, el número de usuarios de estos dispositivos alcanzará 2 billones para 2016 [2]. De tal manera que, los teléfonos inteligentes tienen un rol importante en la vida laboral y personal; ya que no sólo se usan para comunicarse mediante llamadas telefónicas, sino que también gracias a los teléfonos inteligentes es posible reproducir música y videos, tomar fotografías, procesar textos, compartir imágenes, enviar e-mails, navegar en internet, etc. Para este propósito es posible descargar aplicaciones de repositorios oficiales o no oficiales, cuyas funcionalidades se encuentran en un amplio rango; sin embargo, la mayoría de ellas requieren acceso a internet y como consecuencia, los dispositivos están expuestos a los efectos de amenazas como malware u otros riesgos concernientes a la ciberseguridad.

En la actualidad, existen distintos tipos de malware dirigido a teléfonos inteligentes: caballos de Troya, gusanos, virus, adware, ransomware, etc. Los caballos de Troya se catalogan como la amenaza mucho más frecuente ocupando el 85% de las amenazas detectadas [3]. Cabir fue el primer gusano para teléfonos inteligentes reportado en 2004 [4]. Las consecuencias del malware o virus pueden ir desde duración reducida de la batería, anuncios no deseados, degradación del funcionamiento, robo de información personal (cuentas bancarias, agenda telefónica, etc.) hasta el robo de identidad.

Debido a los enormes daños potenciales que puedan ser causados por el malware, se han propuesto muchos modelos para describir el proceso dinámico de propagación de malware. Los objetivos de estos modelos de propagación se pueden clasificar en los siguientes categorías: (1) obtener una comprensión profunda de los mecanismos de propagación mecanismos de malware; (2) predecir la escala del contagio de malware antes de que realmente ocurre; (3) (4) caracterizar la dinámica de infección del malware; y (5) diseñar y evaluar el funcionamiento de las contramedidas para frenar la propagación del malware.

En los últimos años se han desarrollado diversas investigaciones de propagación de malware en teléfonos inteligentes que se enfocan predominantemente en modelar la propagación de malware mediante el uso de teorías de epidemia clásicas debido a la fuerte semejanza en los desempeños de la auto-replicación y la propagación de malware de dispositivos móviles con el desempeño de propagación de los virus biológicos. Particularmente, el uso de los modelos basados en ecuaciones diferenciales ordinarias para describir la mecánica de propagación de malware tipo gusano es muy popular, es posible encontrar diversos modelos basados en alguna versión de SI, SIS, o SIR [5] [6] [7]. Aunque estos modelos continuos tienen una base matemática sólida que permite un estudio cualitativo muy detallado, sin embargo, estos modelos tienen algunas carencias:

- No consideran las interacciones locales entre los teléfonos inteligentes: tasa de infección, tasa de recuperación, etc.
- Consideran que los nodos que forman la red son dispositivos homogéneos y todos pueden conectarse entre sí sin ninguna restricción. El análisis del sistema solo se da en forma macroscópica.
- No son capaces de simular la dinámica individual de cada teléfono inteligente en la red.

Es por ello que, en los últimos años, nuevos modelos que combinan conceptos de matemáticas discreta, física estadística y ciencias de la computación han surgido como una alternativa a los modelos continuos [8]. Uno de tales paradigmas que se han introducido recientemente para emular la propagación de virus y gusanos en teléfonos inteligentes a través de antenas Bluetooth son los Autómatas Celulares (AC) [9-13], sin embargo, la mayoría de los modelos de AC existentes en la literatura también carecen de algunas características importantes en el estudio del comportamiento de ambientes reales, tales como la movilidad de los dispositivos. Además, los modelos consideran que la población de teléfonos inteligentes es homogénea, es decir, con características operacionales semejantes y de seguridad semejantes, y que la transmisión del gusano se realiza en un sólo paso de tiempo, lo que se aleja del desempeño real. Recientemente, Martín del Rey et. [9] propusieron un modelo de AC que toma en cuenta distintos tipos de sistemas operativos y movilidad de los dispositivos al usar dos AC bidimensionales; sin embargo, a pesar de ser una mejor aproximación a las características de un ambiente real, aún tiene algunas limitaciones como el caso en el que la transmisión del gusano es interrumpida por cuestiones de movilidad de los dispositivos. Particularmente, el estudio se realiza en espacios geográficos extremadamente pequeños y los parámetros de entrada empleados en las simulaciones son asignados sin tomar en cuenta comportamientos reales.

Con base en lo anterior, el objetivo de este trabajo de tesis se enfoca en proponer un modelo basado en el paradigma de autómatas celulares y modelos epidemiológicos compartimentales para simular la propagación espacio-temporal de malware de tipo gusano a través de conexiones Bluetooth en

teléfonos inteligentes. De tal manera que, el nuevo modelo tome en cuenta aspectos relevantes en el estudio del tema y que no han sido considerados en otros modelos existentes en la literatura, tales como: los efectos de la resistencia al gusano por características inherentes a un tipo de población (por ejemplo, tipo de sistema operativo), estudio de un área geográfica de cualquier tamaño, movimiento de los dispositivos dentro del espacio geográfico establecido para el análisis de las conexiones interrumpidas y su repercusión en la dinámica de propagación del malware cuyo vector de infección son antenas Bluetooth. Además se busca que el modelo sea computacionalmente simple y adecuado para su uso en predicción. No se consideran medios de propagación como SMS, MMS, P2P, etc.

Para mostrar y validar la efectividad del modelo propuesto, se realizan simulaciones computacionales del mismo junto con análisis numérico de los resultados obtenidos bajo diferentes casos de estudio y distintos parámetros de entrada; como son velocidad de propagación del gusano en función de la densidad de dispositivos, efectos del radio de transmisión de la antena, impacto de la interrupción de las conexiones a consecuencia de la movilidad de los dispositivos, etc.

El resto de este trabajo de tesis se organiza de la siguiente manera. En el capítulo 1, se introduce al lector en los términos relacionados con el trabajo de tesis para un mejor entendimiento y comprensión del mismo. El capítulo 2, se presenta una breve revisión de trabajos relacionados con este trabajo de tesis. Además se proporciona una descripción detallada de la definición de los Autómatas Celulares. Entonces, en el capítulo 3 se presenta un modelo nuevo para describir la propagación de malware tipo gusano en teléfonos inteligentes a través de Bluetooth. Una validación y verificación del desempeño del modelo mediante simulación computacional, se presenta en el capítulo 4. Resultados de simulación del modelo para diferentes valores de los parámetros y para diferentes casos de estudio son presentados. Finalmente, en el capítulo 5 se presentan las conclusiones de este trabajo de tesis y algunas propuestas para trabajo futuro.

Capítulo 1: Malware y Redes Bluetooth

En este capítulo se definirán los conceptos y terminología requeridos para que el lector entienda este trabajo de tesis, en principio se definen los conceptos de Malware tipo gusano y redes Bluetooth como medio de propagación, que ayudaran a tener una mejor comprensión de la descripción de los antecedentes de este trabajo presentados en el capítulo 2.

1.1 Introducción

El Internet como una red de computadoras que interconectan millones de dispositivos de cómputo a lo largo de todo el mundo [1]. En los últimos años, dispositivos finales no tradicionales de Internet como laptops, teléfonos inteligentes, automóviles, sensores ambientales, sistemas de seguridad, etc. están siendo conectados a Internet con el propósito de intercambiar información de cualquier tipo. Cada día vemos más dispositivos de este tipo como herramienta de venta, catálogo de producto, herramienta de gestión de siniestros o contratos, o simplemente como instrumento de uso recreativo. Este hecho aunado al consumismo por estos dispositivos y fenómenos como el BYOD (Bring Your Own Device) han alterado las necesidades de las empresas, tanto a nivel del área de tecnología de información como de los usuarios finales. Particularmente, la proliferación de teléfonos inteligentes (smartphone en inglés) se ha incrementado a un ritmo vertiginoso; de acuerdo al Telegraph, el número de usuarios de estos dispositivos alcanzará 2 billones para 2016 [2].

Un teléfono inteligente es un tipo de teléfono móvil que se construye sobre una plataforma informática móvil, con una capacidad de almacenar datos y realizar actividades, semejante a la de una minicomputadora, y que cuenta con una conectividad mayor que la de un teléfono móvil convencional. Los teléfonos móviles han ido evolucionando hasta tener prácticamente las mismas funcionalidades que una computadora personal. Hoy en día pueden tener agenda, GPS, cámara de fotos, antena Bluetooth, Wi-fi, navegadores web, correo electrónico, acceso a redes sociales, aplicaciones, reproductor de videos y música. Y lo más importante, se almacenan una gran cantidad de datos personales en ellos. Esta expansión del mercado de los últimos años, ha generado que los teléfonos inteligentes sean también un objetivo atractivo para los escritores de software malicioso o malware y por lo tanto, ha motivado el desarrollo de modelos matemáticos orientados a entender, analizar y evaluar las medidas de control de su propagación mediante los diferentes medios de transmisión de información con los que se cuenta.

1.2 Medios de Transmisión Alternativos

Los teléfonos inteligentes no sólo se encuentran conectados a Internet gracias a los planes de datos de los ISPs (Internet Service Provider, por sus siglas en inglés) o puntos de acceso fijos que cubren determinada área, como las redes WiFi, que les permiten consumir servicios en la Web. Otra alternativa es el intercambio de información a través de tecnologías inalámbricas como redes Ad-hoc.

1.2.1 Redes Ad-hoc

Una red Ad-hoc es una red que no posee un control central ni tiene salida a Internet. Esta red es formada "al vuelo" por dispositivos móviles que se encuentran en determinada proximidad o dentro de cierto rango uno del otro, teniendo la necesidad de establecer comunicación entre ellos pero sin contar con una infraestructura de red preexistente en su ubicación [1].

El término *conectividad Ad-hoc* se refiere tanto a la habilidad de un dispositivo de asumir la funcionalidad de maestro o esclavo en una transmisión y a la facilidad con la que los dispositivos pueden unirse o abandonar una red existente. Actualmente, el término Ad-hoc no es nuevo como tal, pero el escenario, el uso y los participantes sí lo son. En el pasado, la noción de redes Ad-hoc frecuentemente era asociada con la comunicación en los campos de batalla y en áreas de desastre; ahora, forma parte de nuevas tecnologías como Bluetooth [10].

Las principales características de las redes Ad-hoc [11] se listan a continuación:

- Topología dinámica. La estructura de la red cambia en el tiempo y por lo tanto, la posición de los nodos. La Fig. 1.1 muestra la movilidad de los nodos, por ejemplo, dicha movilidad cambia la conectividad entre los nodos en función de la distancia que hay entre ellos, las características del espacio geográfico en el que están desplegados y la energía de cada uno de ellos.

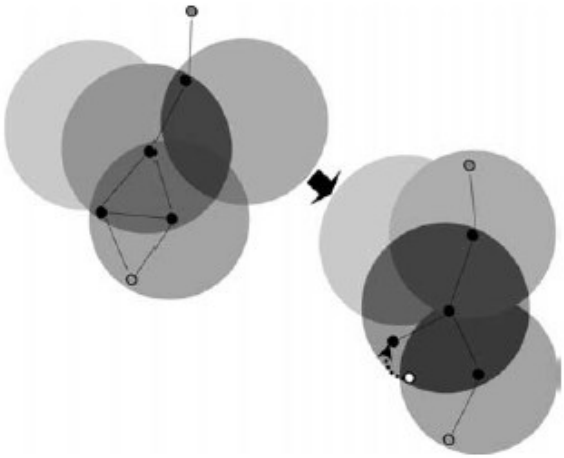


Fig. 1.1 - Topología Dinámica de una red Ad-hoc

- Los nodos que la componen la red son capaces de cambiar el rango de su transmisión.
- Cada nodo de la red actúa como un router independiente.
- Dado el modo de comunicación inalámbrico, los enlaces entre los nodos están restringidos por el ancho de banda y la capacidad variable.
- Existen limitaciones de energía de cada nodo.

1.2.1.1 Bluetooth

Un gran ejemplo de redes Ad-hoc son las redes inalámbricas establecidas entre un teléfono inteligente y distintos dispositivos como impresoras, relojes inteligentes, audífonos, entre otras; llamadas redes Bluetooh. Bluetooth es una tecnología originalmente desarrollada por Bluetooth Special Interest Group (SIG). La tecnología inalámbrica Bluetooth es una tecnología de comunicación de corto alcance destinada a reemplazar los cables que conectan dispositivos móviles o fijos mientras mantenían un alto nivel de seguridad. En 1994 la compañía sueca Ericsson inició el movimiento *Bluetooth Technology* [3]. La intención original era hacer una conexión inalámbrica entre algo similar a unos auriculares y un teléfono. El nombre de Bluetooth está inspirado en la leyenda del rey vikingo danés Harald Blåtand (Harold Bluetooth en inglés) del siglo X. Según la creencia popular, Blåtand tenía una gran habilidad para unir a la gente en negociaciones no violentas. Su destreza con las palabras y la comunicación fue tan lejos como para unir a facciones rivales en lugares que hoy corresponden a Noruega, Dinamarca y Suecia como un sólo territorio. Del mismo modo, la tecnología Bluetooth se creó como un estándar abierto para permitir la conectividad y la colaboración entre los distintos productos e industrias [4] [12].

Por su extensión, una red Bluetooh pertenece a la clasificación de redes WPAN (Wide Personal Area Network, por sus siglas en inglés) definida en el estándar IEEE 802.15.1, cuyo rango de alcance es menor a la de una red LAN, es decir, opera sobre un rango corto y a un bajo consumo de energía. Este tipo de redes opera en la banda sin licencia ISM (Industrial, Scientific, and Medical) a 2.4 GHz. Con ventanas de tiempo de 625 microsegundos. Durante cada ranura de tiempo, el emisor transmite en uno de los 79 canales, cada canal cambia de una forma conocida pero pseudo aleatoria de ranura a ranura. Esta forma de cambio de canales es conocida como frequency-hopping spread spectrum (FHSS) que es capaz de alcanzar tasas de transmisión de hasta 4 Mbps [13].

1.2.1.2 Estructura de una red Bluetooth

Una red Bluetooth se organiza en primera instancia en una red de hasta ocho dispositivos denominada Piconet, la cual designa a uno de los dispositivos como maestro y al resto como esclavos; como se muestra en la Fig. 1.2. El nodo maestro es el que gobierna la Piconet, su reloj coordina el tiempo dentro de la Piconet y sólo puede transmitir datos a un nodo esclavo en cada ranura de tiempo impar. Así, los nodos esclavos pueden transmitir datos sólo después que el nodo maestro se haya comunicado con ellos (ranura de tiempo par).

Adicionalmente a los nodos esclavos, también pueden existir hasta 255 dispositivos *estacionados* en la red. Estos dispositivos no pueden comunicarse hasta que su estatus haya sido cambiado de estacionado (parked) a activo (active) por el nodo maestro. Los estados de un dispositivo Bluetooth serán detallados más adelante en este capítulo.

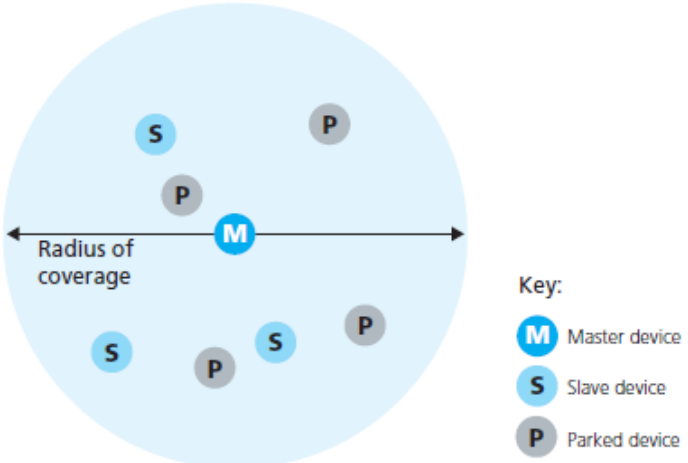


Fig. 1.2 – Ejemplo de una Piconet Bluetooth

Al igual que una piconet donde varios dispositivos Bluetooth son capaces de conectarse uno con otro en forma de red Ad-hoc, múltiples piconets pueden conectarse entre sí para formar redes más grandes llamadas Scatternets. Los dispositivos Bluetooth deben tener capacidad de conexión punto-multipunto para poder establecer la comunicación dentro de la scatternet. Varias piconets pueden comunicarse entre sí a través de una scatternet. Además, un sólo dispositivo Bluetooth puede participar como esclavo en varias piconets pero sólo puede actuar como maestro en una piconet [14] como se muestra en la Fig. 1.3.

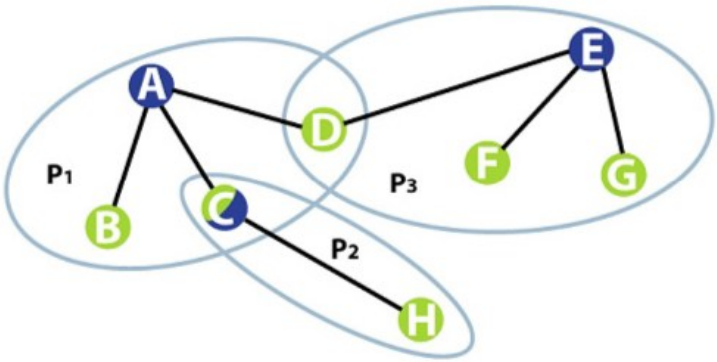


Fig. 1.3 – Ejemplo de Scatternet Bluetooth

La Fig. 1.3 muestra un ejemplo de una scatternet que se compone de tres piconets distintas, P_1, P_2 y P_3. Cada piconet es controlada por un nodo maestro (A, C, E) y contienen uno o más nodos esclavos.

En el caso concreto del nodo C, que conecta a P_1 con P_2, es esclavo en la piconet P_1 y maestro en la piconet P_2.

1.2.1.3 Direcciones y Nombres de Dispositivos

Cada dispositivo tiene una dirección única de 48-bits, es decir, la dirección MAC, comúnmente abreviada como BD_ADDR. Usualmente, este dato será presentado en forma de 12 dígitos hexadecimales. La mitad más significativa (24 bits) de la dirección corresponde a un identificador único del fabricante (OUI por sus siglas en inglés Organization Unique Identifier). La mitad menos significativa corresponden al identificador único del dispositivo Bluetooth.

Los dispositivos Bluetooth también pueden mostrar nombres amigables para el usuario final que son empleados en vez de la dirección MAC para ayudar de manera más efectiva en la identificación del dispositivo. La Fig. 1.4 muestra un ejemplo:

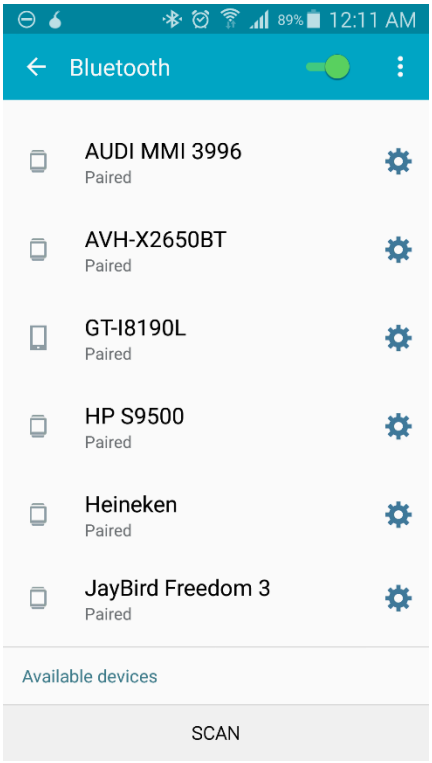


Fig. 1.4 - Dispositivos Bluetooth identificados por un nombre amigable al usuario

Las reglas para la asignación de los nombres son menos estrictas. Los nombres de los dispositivos pueden tener una longitud de 248 bytes y dos dispositivos pueden tener el mismo nombre. En algunas ocasiones, los dígitos de la dirección única del dispositivo son incluidos en el nombre para diferenciar entre uno y otro.

1.2.1.4 Proceso de Conexión

Para establecer una conexión entre dos dispositivos se realiza un proceso de múltiples etapas que se conforma de tres estados progresivos. Se asume que los dispositivos tienen habilitada la antena Bluetooth y la configuración de seguridad permite que sean descubiertos:

1. Indagación (Inquiry). Si dos dispositivos que no tienen conocimiento mutuo, uno debe iniciar un proceso de indagación para intentar descubrir al otro. Un dispositivo envía una solicitud de indagación, cualquier dispositivo a la escucha de ese tipo de peticiones responderá con un paquete que contiene su dirección MAC, posiblemente su nombre y otros datos adicionales.
2. Paginación/Conexión (Paging). La paginación es el proceso de formar una conexión entre dos dispositivos. Antes de que la conexión pueda ser iniciada, cada dispositivo requiere conocer la dirección del otro (este dato es obtenido en la fase de indagación).
3. Conexión (Connection). Después de que un dispositivo ha concluido el proceso de paginación, entra en el estado de conexión. Mientras está conectado, un dispositivo puede participar activamente en la transmisión o puede ser puesto en un estado de ahorro de energía.
    - Modo Activo (Active Mode). Este es el estado regular de un dispositivo conectado en el cual se transmite o recibe datos activamente.
    - Modo de Husmeo (Sniff Mode). Es un modo de ahorro de energía en el que el dispositivo es menos activo. Entrará en espera y sólo escuchará las transmisiones en un intervalo definido. Por ejemplo, cada 100 ms.
    - Modo de Retención (Hold Mode). El modo de retención es temporal y de igual manera es un estado de ahorro de energía en el que el dispositivo regresa a su funcionamiento después de un intervalo de tiempo. La principal diferencia con el modo de husmeo es que el dispositivo con el rol de maestro puede ordenar al esclavo entrar en modo de retención.
    - Modo Estacionado (Parked Mode). Este es el modo de ahorro de energía más profundo. El dispositivo con rol de maestro ordena al dispositivo esclavo que se “estacione” para que permanezca inactivo hasta que el maestro le indique que se active nuevamente.

1.2.1.5 Enlace y Emparejamiento

Cuando dos dispositivos comparten cierta afinidad el uno con el otro, pueden ser enlazados. Los dispositivos enlazados automáticamente establecen una conexión siempre que se encuentren en un rango de transmisión adecuado para alcanzarse. Por ejemplo, cuando un automóvil equipado con una antena Bluetooth es encendido, un teléfono inteligente inmediatamente se conecta al sistema Bluetooth del vehículo dado que ya están enlazados, de modo que ya no es necesaria la interacción del usuario.

Los enlaces son creados en un proceso que se ejecuta una sola vez llamado emparejamiento. Cuando los dispositivos Bluetooth se emparejan, comparten sus direcciones MAC, nombres, perfiles y otra información adicional para almacenarla en sus respectivas memorias. Usualmente, el proceso

de emparejamiento requiere de un mecanismo de autenticación en el que el usuario debe validar la comunicación entre los dispositivos. Este proceso varía dependiendo de las capacidades de los dispositivos involucrados.

1.3 Breve historia de los Virus Computacionales

El término Virus computacional fue introducido por primera vez en 1984 por el matemático Dr. Frederick Cohen, convirtiéndose así en el *padre* de los virus computacionales con sus primeros estudios acerca de éstos. Cohen empleó este nombre como recomendación de su asesor el profesor Leonard Adleman quien eligió el nombre de las novelas de ciencia ficción [15] [16]. Posteriormente, en 1991, los miembros fundadores del CARO (Computer Antivirus Researchers Organization) Vesselin Bontchev, Fridrik Skulason y Alan Sólomon [17] diseñaron un esquema de nombrado de virus computacionales para su uso en productos de antivirus. Actualmente, el esquema de nombrado del CARO está un poco anticuado en comparación con la práctica diaria pero permanece como el único estándar que la mayoría de empresas fabricantes de antivirus siempre quisieron adoptar.

El término malware proviene de la contracción de software malicioso (malicious software), usualmente se emplea para definir un amplio rango de aplicaciones de software hostiles e intrusivas para el sistema operativo y por ende, para la información del usuario. A pesar de que existen múltiples piezas de software las cuales carecen de un buen diseño de seguridad o que permiten el acceso simple a los usuarios del sistema, el término sólo abarca aquellos programas escritos con el propósito específico de interrumpir el funcionamiento normal de un sistema. Es importante mencionar que las aplicaciones con defectos de seguridad no son consideradas como malware ya que sus defectos y pobre diseño no fueron implementados deliberadamente [18].

El Malware abarca una gran cantidad de aplicaciones dañinas (o potencialmente dañinas), tales como virus, gusanos (worms), puertas traseras (backdoors), caballos de Troya (Trojans), keyloggers, password stealers, script viruses, rootkits, software espía (spyware) e incluso adware. En los primeros años de la industria de tecnologías de la información las amenazas eran clasificadas de forma genérica como virus o caballos de Troya, sin embargo, el rápido crecimiento de la tecnología necesitó un término general para cubrir todas las amenazas mencionadas.

En un inicio el malware fue concebido como parte de bromas, vandalismo o incluso experimentos para demostrar inteligencia artificial. Por ejemplo, el primer gusano de Internet y MS-DOS eran inocuos para la computadora y para el usuario. Estaban diseñados para ser molestos y dar a conocer al mundo el nombre de su creador. Tales aplicaciones pseudo-malignas eran sencillas de eliminar y no representaban una amenaza per se. Más que eso, sus autores no tenían interés en los métodos para ocultar el virus; por el contrario, los utilizaban para presumir de sus logros.

En la actualidad, las cosas han cambiado dramáticamente, los escritores de malware no buscan más la gloria ni el reconocimiento, sino las ganancias financieras. Han empezado a prestar atención extra a los mecanismos para mantener el malware oculto del usuario y de los antivirus con la finalidad de explotarlo lo más posible.

El desarrollo y esparcimiento del malware es un negocio de billones de dólares por año. De acuerdo con el reporte emitido por la compañía de investigación Computers Economics, el daño directo total atribuido al malware alcanzó los $13 billones de dólares en 2006 [19] mientras que el Cibercrimen alcanzó un total estimado de forma conservadora de $375 billones de dólares en 2014 [20]. De aquí la importancia de su estudio y modelación.

1.3.1 Diferencias entre Virus y Gusanos

A pesar de la gran variedad de programas de tipo malware, se ahondara específicamente en el tipo gusano y virus, clasificaciones que comúnmente se emplean de forma indistinta dadas sus similitudes.

1.3.1.1 Virus

Son un tipo de software que puede replicarse a sí mismos de forma silenciosa para infectar un equipo en específico. Dado que los virus están asociados con comportamientos destructivos, el término es empleado de forma incorrecta para definir a múltiples tipos de malware. Dependiendo de su complejidad, el virus puede alterar sus subsecuentes copias para escapar de los algoritmos de detección de cadenas simples de los antivirus. Los virus pueden propagarse a través de Internet o cualquier otra topología de red o por infección de archivos en dispositivos removibles como discos duros, memorias USB o MicroSD.

1.3.1.2 Gusanos

Los gusanos también son programas capaces de replicarse a sí mismos de forma silenciosa para propagarse a través de la red tal como lo hacen los Virus, la principal diferencia radica en que el proceso de replicación de un gusano es completamente automático, de modo que no requieren infectar a algún programa en específico. Su potencial destructivo reside en el hecho de que pueden consumir una gran cantidad de ancho de banda mientras que los virus usualmente modifican, eliminan o corrompen archivos del sistema infectado.

1.4 Propagación de Gusanos en Teléfonos inteligentes vía Bluetooth

Cuando un teléfono inteligente está infectado con malware tipo gusano, se asume que se encuentra constantemente en el estado de indagación. El ciclo de infección comienza con la difusión del mensaje de indagación. Cuando otros dispositivos con la antena Bluetooth encendida y la configuración de seguridad que les permite ser descubribles, responden a la solicitud de indagación, hacen que el dispositivo infectado genere un listado de vecinos. El dispositivo infectado extrae uno

de los vecinos de la lista y establece una conexión como si fuera un dispositivo esclavo. Si la conexión es exitosa, se enviara un archivo infectado al dispositivo susceptible. Entonces, el dispositivo infectado termina la conexión. Durante el proceso de replicación del archivo infectado (gusano) y la desconexión con el dispositivo susceptible existe un contador, cuando el tiempo expira, el dispositivo infectado automáticamente detiene la conexión e intenta el mismo proceso con otro vecino de la lista. Si la lista está vacía, el dispositivo infectado entrara nuevamente en el estado de difusión del mensaje de indagación. Cuando el gusano es ejecutado en el dispositivo susceptible, es infectado y entrara en la fase de difusión del mensaje de indagación para encontrar nuevos vecinos susceptibles. La Fig. 1.5 describe el proceso de propagación del gusano [3] [21].

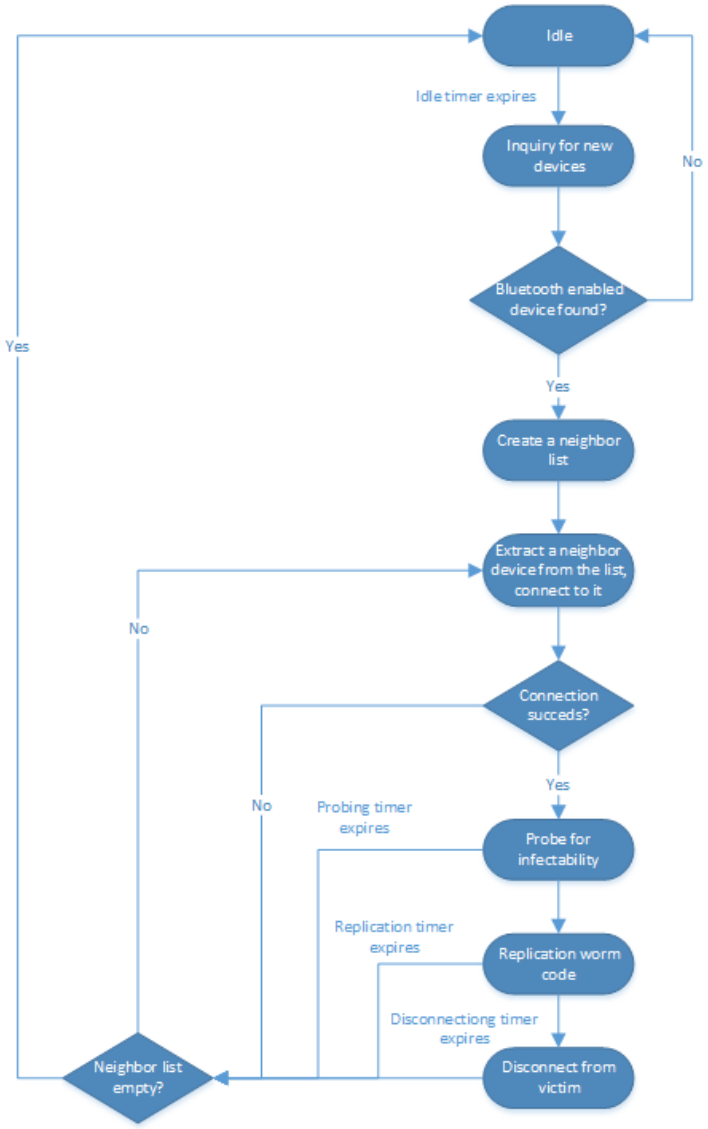


Fig. 1.5 - Ciclo de vida de Infección de un Gusano por Bluetooth.

Debido a los daños potenciales causados por el malware, los investigadores han propuesto diversos modelos para describir el proceso de propagación de esta clase de software, en el que el objetivo del modelado puede ser resumido como:

1. Comprender el comportamiento del software malicioso incluyendo sus atributos y prerrequisitos necesarios para su propagación y factores de influencia.
2. Anticipar la propagación del malware antes de que suceda.
3. Evaluar la accesibilidad del sistema para la propagación de malware y evaluar los impactos de propagación de éste en la red.
4. Identificar las habilidades potenciales del malware para causar actividades dañinas.
5. Detectar la velocidad de propagación del malware y el tiempo requerido para contaminar toda la red.

Con la finalidad de introducir al lector al estado del arte en esta área de estudio que es fundamental para este trabajo de tesis, en el siguiente capítulo, se describen brevemente los modelos existentes principales y sus características.

Capítulo 2: Una Breve revisión de Modelos de Propagación

La aplicación de las matemáticas a la epidemiologıa se remonta al menos hasta el año de 1760 cuando Daniel Bernoulli publicó un tratado sobre la epidemia de peste que en aquel momento afectó Europa. Desde entonces, el interés por la aplicación de las matemáticas al entendimiento y simulación de epidemias ha sido amplio. Debido a que el desempeño de propagación de los gusanos de internet y su auto-replicación son similares a aquellos de los virus biológicos, en los últimos años, el uso de modelos epidemiológicos para analizar la propagación de malware en Internet ha despertado un gran interés en la comunidad científica.

La variedad de amenazas de seguridad causadas por la propagación de malware se ha convertido en un peligro potencial. Esto ha motivado el interés de los autores de software malicioso, que buscan el robo de datos personales, cuentas de banco, acceso a sitios restringidos o cualquier tipo de información sensible y confidencial que se almacena en estos dispositivos. Por lo tanto, la modelación del comportamiento de este tipo de malware se convierte en un tema de importancia en obras recientes. En particular, establecer modelos de propagación de malware se ha utilizado para predecir los efectos secundarios de una nueva amenaza y entender el comportamiento del malware modelado.

En lo siguiente se hace una breve descripción del estado del arte.

2.1 Importancia de los Modelos Epidemiológicos

El mecanismo de transmisión de un individuo infectado a uno susceptible está entendido para casi todas las enfermedades infecciosas, y el esparcimiento de enfermedades a través de una cadena de infecciones también es conocido. Sin embargo, las interacciones de transmisión en una población son bastante complejas, de ahí la dificultad para comprender las dinámicas a gran escala del esparcimiento de una enfermedad sin la estructura formal de un modelo matemático. Un modelo epidemiológico emplea una descripción microscópica (por ejemplo, el rol de un individuo infectado)

para predecir comportamientos macroscópicos del esparcimiento de la enfermedad en la población [22].

En múltiples ciencias es posible realizar experimentos para obtener información y probar hipótesis. Experimentar con la propagación de enfermedades infeccionas en una población humana con frecuencia es imposible, antiético o demasiado costoso. En algunas ocasiones, la información puede ser obtenida de epidemias que surgen de forma natural o de incidencias naturales de enfermedades endémicas, sin embargo, la mayor parte de las veces esta información está incompleta debido a la falta de reporte o documentación de la misma. Esta falta de información confiable hace que los parámetros de estimación no sean tan precisos, de modo que en algunas ocasiones, únicamente se pueden hacer estimaciones sobre un rango de valores para algunos parámetros. Partiendo del hecho de que los experimentos repetibles e información veraz no siempre están disponibles en la epidemiología, los modelos matemáticos y simulaciones computacionales pueden ser empleados para realizar los experimentos teóricos necesarios. Por lo tanto, los modelos epidemiológicos son útiles en la comparación de los efectos de la prevención o en los procedimientos de control.

2.2 Modelos Epidemiológicos Genéricos

La modelación epidemiológica tiene una larga historia en el estudio de las enfermedades biológicas infecciosas. En 1927 [23], 1932 [24] y 1933 [25], Kermack y McKendrick publicaron una serie de artículos titulados “Contributions to the mathematical theory of epidemics”. Dichos artículos son vistos como la base para más investigaciones empleando el modelado matemático (especialmente el determinístico) para explorar la propagación de las enfermedades infecciosas. Los modelos epidemiológicos clásicos incluyen el modelo SI (Susceptible-Infectado), el modelo SIS (Susceptible-Infectado-Susceptible), y el modelo SIR (Susceptible-Infectado-Recuperado) [26].

En general, la población a ser considerada en el estudio es dividida en clases disjuntas las cuales cambian en el tiempo. La clase de individuos susceptibles consiste en aquellos que pueden incurrir en la enfermedad pero que aún no presentan características infecciosas hacia otros individuos susceptibles. La clase de infectados consiste en aquellos que son capaces de transmitir la enfermedad a otros. La clase de removidos o recuperados son aquellos que son depuestos de la interacción susceptibles-infecciosos al recuperarse alcanzando inmunidad hacia la enfermedad, aislamiento o muerte. Las fracciones de la población descrita anteriormente son denotadas por *S*, *I*, y *R*, respectivamente.

En los modelos epidemiológicos el tamaño total de la población se considera constante.

En los modelos SI, SIS, SIR y SIRS los individuos de la población son clasificados de acuerdo al estado de su enfermedad. Estos modelos en su forma básica son mostrados en la Fig. 2.1 (a), (b), (c) y (d). Algunos de los términos para estos modelos se explican a continuación:

- μ denota la tasa de natalidad, que se refiere a la relación entre el número de individuos recién nacidos a través de la población total por unidad de tiempo.

- λ denota la tasa de mortandad, que se refiere a la relación entre el número de infecciones a través del número de muertes debido a la infección en un cierto período de tiempo (generalmente 1 año).
- *N* denota el número total de individuos susceptibles, infectados y recuperados en una población dada.
- *S(t)* es empleada para representar el número de individuos que aún no han sido infectados con la enfermedad en el tiempo *t*, o que son susceptibles a esta.
- *I(t)* denota el número de individuos que han sido infectados por la enfermedad y son capaces de contagiarla a aquellos individuos que se encuentren en la categoría de susceptibles.
- *R(t)* es el compartimento usado para todos los individuos que han sido infectados con la enfermedad y posteriormente se han recuperado. Los individuos en esta categoría no pueden volver a ser infectados ni transmitir la enfermedad a otros.
- β representa el número promedio de contactos directos realizados por un individuo infectado por unidad de tiempo. Se conoce como tasa de contacto o tasa de infección.
- α representa la tasa media de recuperación.
- δ representa la pérdida media de la tasa de la inmunidad de los individuos recuperados o denota la tasa cuando los individuos recuperados nuevamente se vuelven susceptibles a la enfermedad.
- β*SI* representa el número de nuevas infecciones por unidad de tiempo.
- α*I* representa el número de nuevas recuperaciones o denota el número de nuevos individuos susceptibles por unidad de tiempo.
- δ*R* representa el número de nuevos individuos susceptibles por unidad de tiempo.

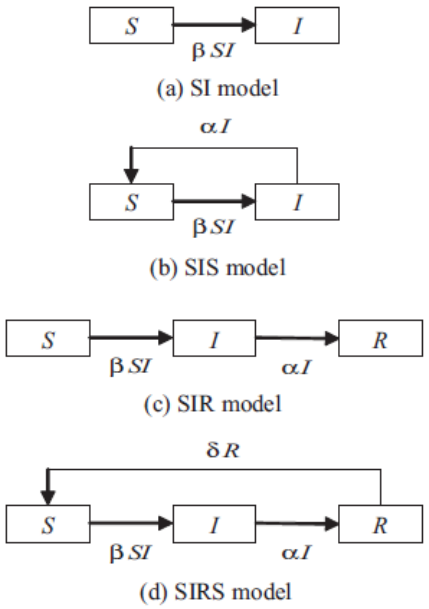


Fig. 2.1 - Modelos Epidemiológicos Determinísticos Básicos

En el modelo SI (Fig. 2.1.a), se supone que un individuo susceptible después de un contacto exitoso con otro individuo infectado, pasa al estado de infectado sin desarrollar inmunidad a la enfermedad. En el modelo SIS (Fig. 2.1.b), se asume que un individuo susceptible después de un contacto exitoso con otro individuo infectado, pasa al estado infectado sin desarrollar inmunidad a la enfermedad. Por lo tanto, después de la recuperación, los individuos infectados regresan al estado de susceptible. En el modelo SIR (Fig. 2.1.c), cuando los individuos se vuelven infectados, desarrollan inmunidad a la enfermedad entrando al estado *R*. El modelo SIR ha sido aplicado a enfermedades características de la infancia tales como varicela, sarampión y paperas. Finalmente, en el modelo SIRS (Fig. 2.1.d), se asume que los individuos infectados pueden recuperarse y nuevamente volverse susceptibles tras la recuperación.

2.3 Clasificación de los modelos para dinámica de propagación

Al igual que en otras disciplinas, el uso de modelos y simulaciones son una gran herramienta que permite estudiar el esparcimiento de enfermedades infecciosas o incendios forestales entre otros fenómenos, del mismo modo, este tipo de herramientas son necesarias en la ciencia de la computación para estudiar el esparcimiento de software malicioso a lo largo de una red de dispositivos, con el objetivo de evaluar la efectividad de las configuraciones de seguridad de la misma y de esta forma poder tomar decisiones bien fundamentadas para contener el esparcimiento o al menos mitigar los efectos dañinos ocasionados.

Como se observó anteriormente, la mayoría de los modelos epidemiológicos existentes están basados en el modelo Kermack-McKendric y pueden ser agrupados en tres grandes categorías [26]: determinísticos, estocásticos y espacio-temporales.

Los modelos determinísticos fueron los primeros en ser empleados y por ende los más populares. Están representados por sistemas de ecuaciones diferenciales donde se asume que el número de individuos susceptibles e infectados es una función definida en el tiempo. Las principales ventajas que ofrecen es que son capaces de describir la dinámica entre las tasas de cambio y el tamaño de la población y la base matemática que los soporta está bien fundamentada haciéndolos aptos para realizar estimaciones precisas. Algunas de sus principales desventajas son que la adición de nuevos parámetros de entrada puede ser complejo, lo que usualmente dificulta su implementación y ejecución al requerir una alta cantidad de recursos computacionales. En el caso de las simulaciones se observa que en fases iniciales no pueden caracterizar con precisión la propagación del malware dado que tienden a iniciar con un número de individuos infectados muy pequeño.

En los modelos estocásticos [26] los individuos son representados por procesos no deterministas. Estos modelos pueden describir las interrelaciones dinámicas empleando distribuciones de probabilidad haciéndolos adecuados para el estudio de poblaciones pequeñas, sin embargo, dada la carencia de un modelo matemático bien formulado, la ejecución de análisis matemático es complicado.

Los modelos espacio-temporales [26] permiten el estudio de sistemas auto-organizables; emplean reglas de interacción local (reglas de transición) para determinar la evolución y descripción de un

sistema complejo de forma simple, sin embargo, estas reglas de transición son vulnerables a la interferencia humana durante el proceso de definición. Dentro de este tipo de modelos se ubican los Autómatas Celulares (AC), que se describen detalladamente en la siguiente subsección y que son el enfoque principal de este trabajo de tesis.

En la Tabla 2.1 se resume un comparativo de las características de los modelos epidemiológicos de propagación.

Tipo	Determinístico	Estocástico	Espacio-temporal
Teoría	Ecuaciones diferenciales	Procesos de Markov	Autómata Celular
Espacio	Continuo	Continuo	Discreto
Tiempo	Continuo	Continuo o discreto	Discreto
Estado individual	Continuo	Discreto	Discreto
Interacción individual	No	No	Sí
Alcance adaptativo	Movimiento aleatorio de los individuos	Un número pequeño de individuos	Un número grande de individuos
Descripción del modelo	Ecuaciones diferenciales	Cadenas de Markov continuas o en tiempo discreto	Reglas de evolución estocásticas

Tabla 2.1 - Modelos básicos para dinámica de propagación

2.4 El paradigma de los Autómatas Celulares (AC)

Como humanidad, creamos nuevos modelos para entender el mundo en el que vivimos desde distintas perspectivas. A finales de la década de 1940, el matemático John Von Neumann comenzó a explorar formalmente la posibilidad de crear máquinas que a su vez pudieran crear máquinas más complejas que ella. Von Neumann observó que de manera análoga en los procesos biológicos las células pueden generar construcciones más complejas, así, el concepto de complejidad en las máquinas puede ser basado en el la idea de la auto-reproducción [27].

Suponiendo que una máquina es capaz de construir una copia de sí misma empleando partes más sencillas encontradas en su ambiente tendrá como resultado una máquina igual de complejidad. La auto-reproducción derriba el supuesto de que las máquinas únicamente pueden crear estructuras más simples a ellas tal como pasa en una ensambladora de autos robotizada (naturaleza degenerativa de la complejidad) como se ilustra de forma artística en la Fig. 2.2.

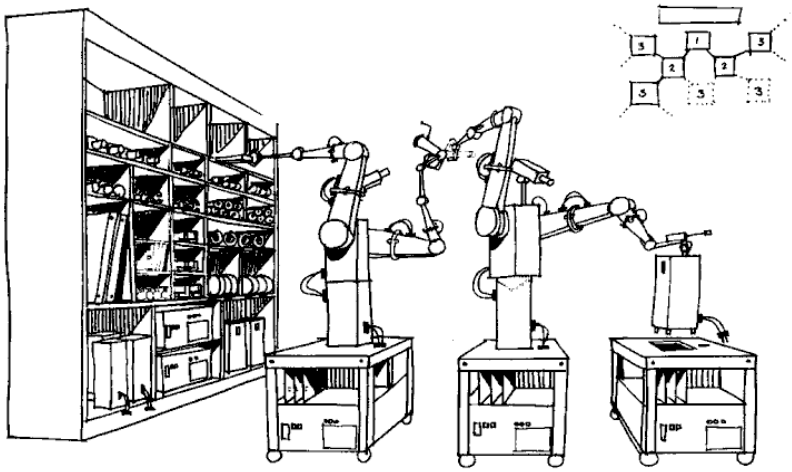


Fig. 2.2 - Demostración propuesta del robot simple de auto-replicación

Una interpretación artística financiada por la NASA del autómata de Von Neumann que produce otros autómatas, el título original es: "Demostración propuesta del robot simple de auto-replicación", basado en la automatización avanzada para las misiones espaciales de la NASA / ASEE

La modelación de esta máquina como una autómata celular fue gracias a la sugerencia de Stanislaw Ulman, ya que Von Neumann notó la dificultad de manejar las características necesarias que la máquina a auto-replicarse debía tener para tomar los elementos necesarios para copiarse del entorno que la rodea, de esta manera, el ambiente de la máquina auto-replicable es un autómata celular (referenciados de aquí en adelante como AC) bidimensional.

Los AC son sistemas dinámicos discretos, cuyo espacio, tiempo y por lo tanto, variables de estado, son discretos. La característica principal es que la dinámica de estos modelos se basa en reglas de interacción local, es decir, estados de las células vecinas, lo que permite considerar aspectos individuales de los entes que conforman el sistema que se simula en forma simple. Dichas reglas son aplicadas de forma iterativa tantas veces sea requerido.

Formalmente, se define a un AC como una tupla $(\mathrm{C}, \Sigma, V, f)$, donde *C* representa el espacio celular, Σ representa el conjunto finito de estados posibles que una célula puede tener, *V* representa el conjunto finito de índices que representan a la vecindad de la célula y *f* representa la función de transición $V \rightarrow \Sigma$ a través de la cual todas las células evolucionan de forma síncrona [28].

Los autómatas celulares están compuestos por los siguientes elementos:

- Espacio Celular. Es la colección de celdas en un espacio. En general, es una rejilla de células regulares de *d*-dimensiones. En la práctica, los espacios celulares son finitos. La Fig. 2.3 muestra algunos ejemplos de espacios celulares.
- Variable de Tiempo. La dinámica del sistema celular se desarrolla a lo largo de un tiempo discreto.
- Estado y conjunto de estados.
  - El estado de las células representa la información que especifica la condición actual de la célula.

- El conjunto de estados es el conjunto de valores aceptables para cada estado de la celda. Con frecuencia se define un estado de inactividad S_0 que representa el estado de inactividad de la célula

- Vecindad. Es el conjunto de células cuyo estado puede influenciar directamente el estado futuro de una célula, se considera la célula misma que es rodeada por la vecindad. Típicamente, la vecindad está formada por un conjunto pequeño de células adyacentes dado que se asume que los sistemas celulares sólo intercambian información localmente. Es posible especificar un radio o rango que comprende a todas las células dentro de él como parte de la vecindad.
- Función de transición. Especifica cómo el estado de una célula se desarrolla en el tiempo. Depende únicamente del estado de las células que pertenecen a la vecindad de la célula en cuestión y, posiblemente, a la posición de la célula en el tiempo. Esta función es determinística y da el estado $S_i(t+1)$ de la i-ésima célula en el paso de tiempo $t+1$ en función del estado de las células en el vecindario.

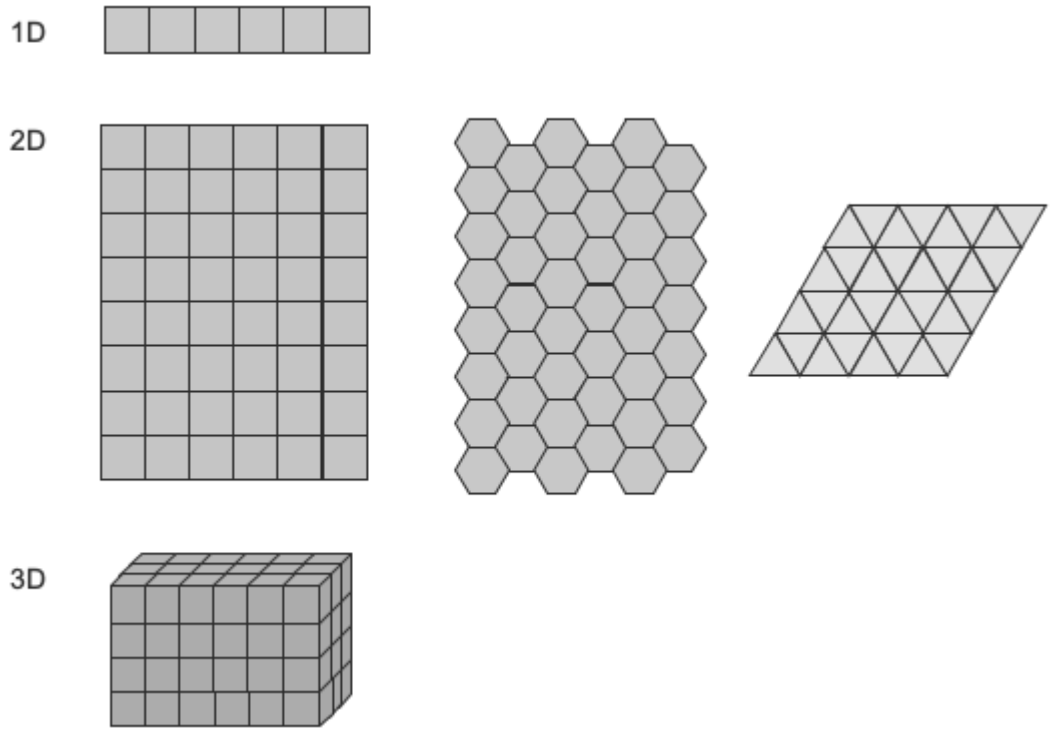


Fig. 2.3 - Espacios Celulares de los AC

- Condiciones de fronteras o Tipos de fronteras. Es la especificación de las condiciones de contorno del espacio celular, ya que de no hacer esto, las células que se encuentran en los extremos pueden carecer de algunas de las células necesarias para formar la zona prescrita. Las tipos de fronteras pueden ser divididos de la siguiente forma:
  - Asignada: Definición de una vecindad virtual. A las celdas virtuales requeridas para completar la vecindad se les puede asignar un estado que no dependa del estado actual del sistema celular como se muestra en la Fig. 2.4:

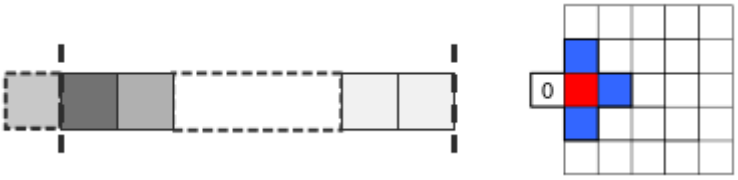


Fig. 2.4 - Frontera Asignada

- Periódica: La solución más simple a la presencia de límites es eliminarlos al transformar el espacio celular de un espacio limitado a uno sin límites como se muestra en la Fig. 2.5:

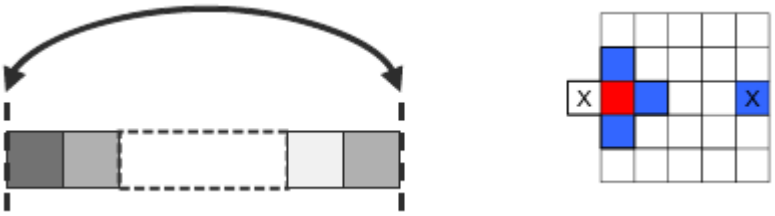


Fig. 2.5 - Frontera Periódica

- Adiabática o de copia: Son aquellos donde a las celdas de una vecindad virtual se les puede asignar un estado que es copia del estado de las celdas del sistema celular, es decir, son especificados al copiar el estado de las celdas de la frontera como se muestra en la Fig. 2.6:

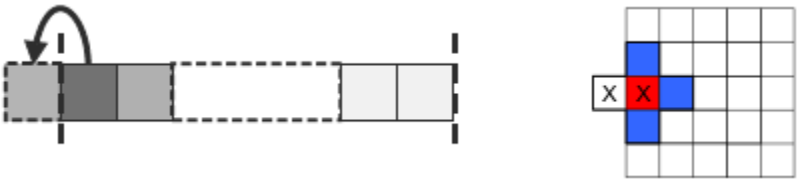


Fig. 2.6 - Frontera Adiabática

- Reflexión: Corresponden a la definición de un proceso que refleja algunos de los fenómenos que son modelados dentro del sistema celular. La definición del proceso de reflexión depende de los detalles de lo que se está modelando. La Fig. 2.7 ilustra el concepto:

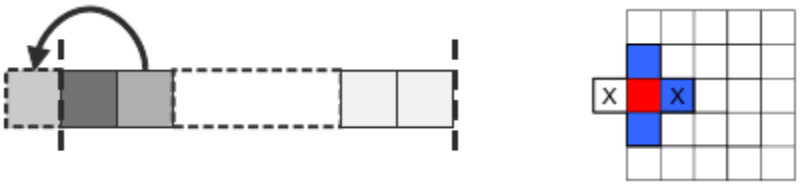


Fig. 2.7 - Frontera de Reflexión

- Absorción: También llamadas de frontera abierta, son clases de fronteras especiales que permiten simular un espacio celular infinito empleando un espacio finito como se muestra en la Fig. 2.8:

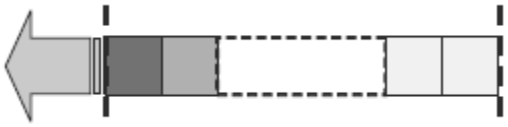


Fig. 2.8 - Frontera de Absorción

Una vez introducido las características de los modelos epidemiológicos de propagación, en la siguiente subsección se presenta un breve estado del arte particularmente enfocado a modelos de propagación en dispositivos móviles mediante Bluetooth, que es tema sobre el que se enfoca este trabajo de tesis.

2.5 Modelos de Propagación de Software Malicioso (Malware)

El software malicioso y su propagación en dispositivos móviles se han estudiado ampliamente en la literatura y un gran número de modelos de propagación de software malicioso se han ya propuesto para estudiar los problemas epidemiológicos en teléfonos inteligentes. Estos modelos y su análisis juegan un papel natural en el entendimiento y predicción de la dinámica de propagación de una infección. Además, las simulaciones computacionales de los modelos proporcionan una herramienta muy útil para el análisis de epidemias reales y ofrecen un método de verificación efectivo del desempeño de los modelos matemáticos. Su aplicación en casos de estudio proporciona también un medio cuantitativo para evaluar la dinámica de propagación de una infección.

Particularmente, es posible encontrar una amplia variedad de trabajos basados en modelos matemáticos para describir la propagación de malware tipo gusano a través de antenas Bluettoth. En lo siguiente, se resumen de manera breve los mismos.

Yan y Eidenbenz [21] propusieron un modelo analítico para estudiar la propagación del malware tipo gusano. El impacto de los patrones de movilidad es analizado al introducir parámetros de entrada tales como el grado promedio de los nodos, la tasa promedio de encuentro de los nodos y la distribución de la duración de la conexión entre ellos.

Rhodes y Nekovee [29] investigaron los efectos de las características de la población y el comportamiento de los dispositivos en la dinámica de propagación de gusanos empleando el modelo SIP. En este modelo, se asume que hay un sólo dispositivo infectado capaz de esparcir un gusano con determinada probabilidad a cualquier dispositivo dentro de su radio de comunicación inalámbrico *R*. Si un gusano es introducido en el sistema, cada dispositivo puede ser susceptible (*S*), infectado (*I*) o recuperado (*P*) de modo que la población se mantiene constante. Sin embargo, Rhodes y Nekovee no consideraron las características espacio-temporales en la dinámica de propagación del gusano, y tampoco consideraron el impacto de las diferencias individuales en la dinámica de propagación de distintos gusanos.

Martin et al. [30] estudiaron la propagación de virus computacionales empleando un modelo SIS. Sin embargo, los autores no consideraron el impacto de las diferencias individuales en la propagación de virus basados en la proximidad entre los dispositivos y de igual manera, tampoco modelaron las características espacio-temporales.

Mickens y Noble [7] propusieron un marco probabilístico de encolamiento para modelar la propagación de virus en dispositivos móviles a través de interfaces inalámbricas de corto alcance. Los autores demostraron el impacto de la velocidad de un nodo en el nivel de infección de una red y ofrecieron una contraparte estocástica a los modelos determinísticos para el modelado de esta clase de virus. Sin embargo, no caracterizaron el impacto de las diferencias individuales en la dinámica de propagación de los virus, al igual que tampoco caracterizaron los detalles espacio-temporales en la dinámica de propagación.

Cheng et al. [5] propusieron un modelo analítico para analizar la velocidad y severidad del esparcimiento de malware hibrido como CommWarrior. Sin embargo, los autores no consideraron las diferencias individuales en la dinámica de propagación del malware, al igual que tampoco consideraron las características espacio-temporales.

Ramachandran y Sikdar [31] presentaron un modelo analítico para explorar el impacto de varios mecanismos de esparcimiento tales como las descargas de internet o redes P2P y transferencias empleando antenas Bluetooth en las redes de teléfonos inteligentes. Sin embargo, Ramachandran y Sikdar no caracterizaron el efecto del comportamiento humano en la propagación del malware.

Xia et al. [32] construyeron un modelo SEIRD (susceptible, exposed, infected, recovered, dormancy) para modelar el esparcimiento del gusano ComWar a través de Bluetooth y MMS. Ellos dividían la cantidad de dispositivos en cinco estados y 11 tipos de conversiones. Sin embargo, los autores no consideraron la variabilidad en la propagación del malware ni tampoco evaluaron el comportamiento humano como parte de la dinámica de propagación del malware.

Peng y Wang [33], [34] propusieron un modelo de propagación denominado WPM. WPM está basado en un AC bidimensional para simular la dinámica de propagación del gusano de un sólo nodo a toda la red. Este modelo integra un factor de infección que evalúa el grado de esparcimiento para los nodos infectados, y un factor de resistencia que ofrece una evaluación de la resistencia del nodo susceptible. Sin embargo, los autores consideran que la transmisión del gusano se realiza en un sólo paso de tiempo además de que los teléfonos permanecen estáticas.

Bakhshi et al. [35] propusieron un modelo de propagación denominado MP-CA. MP-CA está basado en un AC, en el cual se consideraba un estado de reposo en el que el teléfono inteligente agotaba

su batería debido a las constantes búsquedas que realiza y la generación de un histórico de infección entre los dispositivos. Sin embargo, el modelo es aplicado a poblaciones de teléfonos inteligentes bajas (1, 000 dispositivos), consideran que los teléfonos en el espacio celular permanecen estáticos y que sus características son homogéneas.

Martín del Rey et al. [9], [36] propusieron un modelo de propagación denominado SCEIS. SCEIS está basado en dos AC. El primero es un AC bidimensional denominado A_G que controla el espacio celular y a través del cual se obtiene el conteo del número de dispositivos en cada compartimento (susceptible, carrier, exposed, infected, susceptible). El segundo es un AC en grafo denominado A_L. Este AC simula el comportamiento individual de cada teléfono inteligente del sistema. A pesar de que los autores modelaron factores de resistencia, poblaciones heterogéneas, estado de la antena Bluetooth y movimiento de los dispositivos, el modelo es aplicado a espacios bidimensionales sumamente pequeños (5×5 y 10×10) y no se considera la interrupción de la infección del gusano por la movilidad del dispositivo.

La Tabla 2.2 muestra un comparativo entre los modelos mencionados anteriormente

Modelo	Teoría	Diferencias individuales	Comportamiento humano	Movilidad
Yan [21]	ED	No	No	No
SIP [29]	ED	No	No	No
SIS [30]	ED	No	No	No
Mickens [7]	ED	No	No	No
Cheng [5]	ED	No	No	No
Ramachandran [31]	ED	No	No	No
SEIRD [32]	ED	No	No	Sí
WPM [33]	AC	Sí	No	No
MP-CA [35]	AC	Sí	No	No
SCEIS [9] [36]	AC	Sí	Sí	Sí

Tabla 2.2 - Comparativo de modelos enfocados a propagación de malware tipo gusano a través de antenas Bluetooth y sus características
Donde ED denota Ecuaciones Diferenciales, AC denota Autómatas Celulares

Como se aprecia en la tabla anterior, los modelos basados en la teoría de AC junto con modelos epidemiológicos compartimentales, ofrecen grandes beneficios en el modelado de la dinámica de propagación del malware al permitir modelar interacciones locales entre los dispositivos, comportamiento humano que determinan el contacto efectivo del gusano al aceptar o rechazar las transmisiones de archivos, entre otros.

En el siguiente capítulo se introduce un modelo nuevo basado en el paradigma de AC para la propagación de software malicioso mediante antenas Bluetooth. La dinámica del modelo se basa en aquella de los modelos epidemiológicos determinísticos compartimentales y se ajusta para representar la propagación espacio-temporal del malware. El modelo toma en cuenta aspectos importantes para la propagación de malware en teléfonos inteligentes a través de Bluetooth, que a la fecha no se han considerado por otros modelos de AC existentes.

Capítulo 3: Un modelo de propagación de Gusanos basado en AC

En este capítulo, se introduce un modelo nuevo basado en el paradigma de autómatas celulares y modelos epidemiológicos compartimentales para simular la propagación espacio-temporal de malware de tipo gusano, a través de conexiones Bluetooth en teléfonos inteligentes. De tal manera que, el nuevo modelo toma en cuenta aspectos relevantes en el estudio del tema y que no han sido considerados en otros modelos existentes en la literatura, tales como: los efectos de la resistencia al gusano por características inherentes a un tipo de población (por ejemplo, tipo de sistema operativo), estudio de un área geográfica de cualquier tamaño, movimiento de los dispositivos dentro del espacio geográfico establecido para el análisis de las conexiones interrumpidas y su repercusión en la dinámica de propagación del malware. El modelo toma en cuenta en su definición un factor fundamental en la propagación de cualquier virus computacional, la movilidad de los teléfonos.

El modelo presentado en este trabajo está basado en el uso de un AC probabilístico que se emplea para controlar la dinámica del sistema entero. El modelo preserva la simplicidad computacional que caracteriza a los modelos basados en AC y a la vez representa de manera más fiel el comportamiento de propagación del gusano en el espacio y el tiempo.

3.1 Formulación del Modelo

El modelo consiste de un AC probabilista bidimensional definido en una sola capa o espacio celular denotada por *A*, donde cada célula puede estar ocupada o no por un agente que emula a un teléfono inteligente cuyas variables de estado cambian en el tiempo (ver la Fig. 3.1). El espacio *A* se define por un arreglo bidimensional de $L \times M$ células (como se muestra en la Fig. 3.2) de la siguiente manera:

$$A = \{(i,j) \mid i,j \in \mathbb{Z}, -L \leq i \leq L, -M \leq j \leq M\}$$

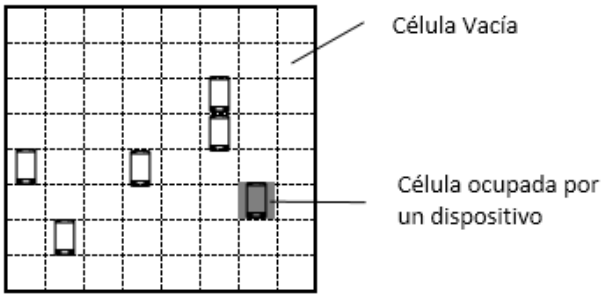


Fig. 3.1 - Teléfonos inteligentes desplegados en el Espacio Celular

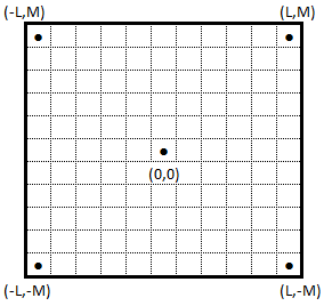


Fig. 3.2 - Dimensiones del Espacio Celular

Dada la tendencia de sobre estimación en la evaluación de conexiones entre dispositivos observada en el planteamiento del estudio del área geográfica, es necesario establecer límites en ella. La delimitación del espacio se hace mediante una de las características propias del AC: las Fronteras. Las fronteras (descritas anteriormente) acotan el alcance que forman las vecindades de las células que se encuentran en los bordes del área geográfica de estudio.

Estas vecindades representan el establecimiento de conexiones en una red de dispositivos con antenas Bluetooth (Piconets) que se realizan de forma dinámica entre dispositivos que se encuentran en un cierto radio de transmisión del dispositivo maestro. La modelación de los dispositivos que están dentro del radio de alcance de otro que desea iniciar una transmisión, se establece mediante el uso de una vecindad de Moore de radio *r* mostrada en la Fig. 3.3 respectivamente, donde *r* denota el alcance de transmisión de la antena. El número de vecinos en una vecindad de Moore es calculado como $(2r+1)^2 - 1$.

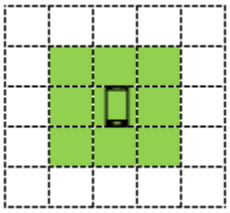


Fig. 3.3 - Vecindad de Moore de r = 1

Para definir la dinámica del modelo, se toma en cuenta las características de propagación del gusano a través de Bluetooth, de tal manera que el estado epidémico de un teléfono inteligente se divide en siete compartimentos que se describen a continuación:

Susceptible (S)	Dispositivos saludables que son vulnerables al contagio del gusano si están en el radio de transmisión de un dispositivo infectado.
Expuesto (E)	Dispositivo susceptible que está conectado con un dispositivo infectado el cual le está enviando copia del gusano. Los dispositivos expuestos no son capaces de iniciar contagios hasta que tengan una copia completa del gusano.
Portador (C)	Dispositivos a los que les fue enviada una copia completa del gusano pero su sistema operativo no corresponde al sistema

	operativo para el cual fue diseñado, evitando que el gusano entre en operación y como consecuencia evitando que se propague. Este estado es un estado terminal.
Infectado (I)	Dispositivos que cuentan con una copia completa y funcional del gusano la cual está en operación. Los dispositivos infectados pueden contagiar a otros dispositivos susceptibles hallados en su vecindad (rango de transmisión).
Diagnosticado (D)	Estado del teléfono inteligente en el cual se identificó el tipo de gusano y se tomará una acción reactiva para intentar eliminarlo.
Recuperado (R)	Dispositivos a los cuales el gusano les fue removido de forma permanente dándoles inmunidad ante un nuevo contagio del mismo malware al instalar una vacuna de antivirus. Este estado es un estado terminal.
Interrumpido (INT)	Dispositivos expuestos que estuvieron conectados con un teléfono inteligente infectado y por cuestiones de movilidad salieron del rango de transmisión de la antena Bluetooh del dispositivo infectado en el tiempo t antes de finalizar la transferencia del gusano. Estos dispositivos regresaran al estado Susceptible al tiempo $t + 1$.

El proceso de transformación de los estados para la propagación del gusano es mostrado en la Fig. 3.4.

Sea $\omega_{ij}^{u}(t)$ que denota el estado de un teléfono inteligente *u* localizado en la célula con índices (*i, j*) en el tiempo *t*, entonces $\omega_{ij}^{u}(t) \in \{S, E, C, I, D, R, INT\}$.

Sea *N* el número teléfonos inteligentes que existen en el espacio celular, cuyo rango de comunicación es *r*. Sea el número de susceptibles, expuestos, portadores, infectados, diagnosticados, recuperados e interrumpidos al tiempo *t* denotados por *S(t), E(t), C(t), I(t), D(t), R(t) e INT(t)*, respectivamente.

Por consiguiente, la población total *N* de teléfonos inteligentes es definida como

$$N = S(t) + E(t) + C(t) + I(t) + D(t) + R(t) + INT(t) \qquad (3.1)$$

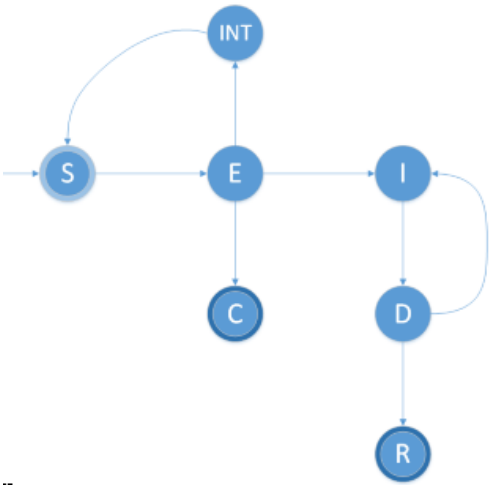


Fig. 3.4 – Relación de la transición de estado para la propagación del gusano

La representación de cada teléfono inteligente *u* localizado en la célula *i,j* del espacio celular se hace mediante el uso de un agente, cuyos atributos característicos se describen en la Tabla 3.1.

Atributo	Variable	Descripción
Tipo de Sistema operativo	*TipoSO*	Corresponde al sistema operativo instalado en el teléfono inteligente, los tipos considerados son Android, iOS y Windows Mobile. El funcionamiento del gusano dependerá completamente del tipo de sistema operativo.
Estado actual	$\omega_{i,j}^{u}(t)$	Estado o compartimento al que el teléfono inteligente pertenece en el tiempo t. Las evaluaciones de la función de transición emplearán éste valor y darán como resultado el Estado Siguiente.
Estado siguiente	$\omega_{i,j}^{u}(t+1)$	Estado al que el teléfono inteligente cambiará en el tiempo $t+1$ en base a la función de transición definida y del estado actual de los teléfonos inteligentes vecinos.
Conectado con	*ConectadoCon*	Identificador del teléfono inteligente infectado con el que se encuentra conectado en el tiempo t. El dispositivo actual sólo puede establecer una conexión por ciclo de tiempo.
Tiempo inicio de infección	TTI	Tiempo en el que el teléfono inteligente pasó del estado Susceptible a Expuesto. El tiempo de inicio será considerado en $t+1$ ya que primero se acepta la transmisión del gusano y posteriormente se inicia la transferencia. Este atributo será usado para llevar el registro del total de ciclos de tiempo que un teléfono inteligente Infectado debe mantenerse

		dentro de la vecindad de un teléfono inteligente Expuesto para completar la transferencia del gusano.
Infectado por	InfectPor	Identificador del teléfono inteligente Infectado con el que se mantuvo la conexión durante todo el periodo de latencia requerido para la transmisión del gusano y que provocó que el estado siguiente del dispositivo actual pase de Expuesto a Infectado.
Dirección de movimiento	DirMov	Punto cardinal hacia el que el teléfono inteligente intentara moverse en cada paso de tiempo.

Tabla 3.1 - Atributos del Agente Teléfono inteligente

3.1.1 Dinámica de movilidad

El modelo introduce en su definición la movilidad de los teléfonos inteligentes a lo largo del espacio celular *A*. Para ello, cada instante de tiempo cada uno de los teléfonos inteligentes existentes en el espacio celular puede moverse a una de sus células vecinas en la vecindad de Moore (como se muestra en la Fig. 3.5). Como ya se mencionó, el modelo que se propone considera la movilidad de los dispositivos en su definición. Así, a cada teléfono inteligente existente en la región geográfica, se le asigna de inicio una dirección para moverse: Norte (N), Sur (S), Este (E), Oeste (O), Noroeste (NO), Noreste (NE), Sureste y Suroeste (SE). Entonces, en los pasos de tiempo subsecuentes un teléfono se mantiene moviéndose en esa misma dirección, con probabilidad uniforme P_{Mov}, siempre que le sea posible (la celda objetivo esté desocupada, ver la Fig. 3.6). Cuando un movimiento en un instante de tiempo *t* a la celda destino ya no es posible, porque se encuentra ocupada, el dispositivo no se mueve y se le reasigna de manera aleatoria una nueva dirección de movimiento que usará a partir del siguiente instante de tiempo $t + 1$ (ver la Fig. 3.7) y siguiendo el proceso previamente descrito.

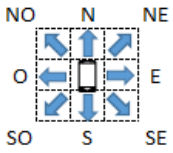
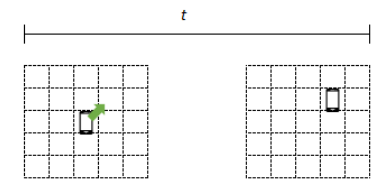
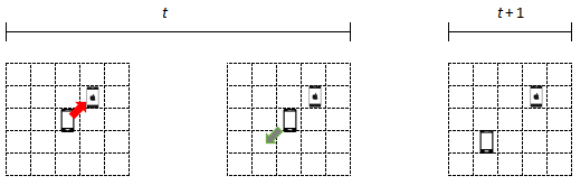


Fig. 3.5 - Posibles Direcciones de Movimiento de un Teléfono inteligente



(a) Validación de disponi - bilidad de la célula destino (b) Avance del smarphone en la dirección elegida durante el mismo ciclo de tiempo

Fig. 3.6 - Movimiento del Teléfono inteligente cuando la célula destino está libre



(a) Detección de célula des - tino ocupada (b) Selección de una nueva dirección de avance (c) Avance a la nueva dirección calculada

Fig. 3.7 - Recalculo de una nueva dirección de movimiento en el tiempo t y avance en el tiempo t + 1

3.1.2 Consideraciones Generales

- El modelo que se propone considera únicamente como vector de infección las conexiones Bluetooth.
- No se considera la pila del protocolo Bluetooth (cabeceas, tamaño de paquetes, etc.) en las funciones de transición del modelo. Únicamente se modela la mecánica de comunicación mediante este protocolo.
- Se considera una población de teléfonos inteligentes heterogénea, es decir, con diferente sistema operativo y configuraciones de seguridad. Sin embargo la definición de la dinámica es semejante para toda la población.
- La población de teléfonos inteligentes es constante en el tiempo.
- La población de teléfonos inteligentes perteneciente a un estado epidémico particular es una cantidad entera, no se consideran poblaciones fraccionarias.
- La forma de infección es de un teléfono inteligente infectado a otro teléfono inteligente “sano”. Para que la infección sea exitosa, el dispositivo sano deberá mantenerse en el rango de transmisión del teléfono inteligente infectado durante todo el tiempo requerido para la transmisión del gusano (tiempo de latencia).
- Un teléfono inteligente expuesto solo puede estar conectado con un solo teléfono inteligente infectado en el tiempo *t* y viceversa.
- Un teléfono inteligente que fue infectado y posteriormente recuperado, adquiere inmunidad definitiva al gusano. Se asume que se instaló una vacuna ante ese tipo de código malicioso en particular. En caso de existir conexión con un teléfono inteligente expuesto, ésta será cancelada haciéndolo pasar al estado INT.
- Únicamente los teléfonos inteligentes susceptibles podrán ser infectados.
- Los teléfonos inteligentes en el estado de INT pasarán al estado Susceptible en el tiempo $t + 1$.
- El modelo evoluciona en pasos de tiempo *t* equivalentes a 1 segundo.
- No se considera la interrupción de la propagación del gusano como consecuencia de agotamiento de la batería de los teléfonos inteligentes infectados.

3.2 Dinámica General del Sistema

La modelación de la dinámica de propagación del gusano se divide en cuatro procesos macro descritos a continuación y mostrados gráficamente en la Fig. 3.8. Los procesos 2 a 4 son ejecutados en cada paso de tiempo *t* hasta que el criterio de finalización de la prueba se cumple:

1. **Asignación de los teléfonos inteligentes al espacio celular**: Asignación de los valores iniciales del espacio celular y parámetros globales e individuales de los teléfonos inteligentes. En este proceso, se asigna la cantidad de dispositivos infectados.
2. **Ejecución del proceso demográfico:** Ejecución de los cálculos correspondientes para determinar la nueva ubicación de cada teléfono inteligente en el espacio celular *C* si es que se cumplió con la probabilidad P_{MOV}. Todos aquellos dispositivos a los que se haya calculado una célula vacía se moverán a ella en ese instante de tiempo *t*.
3. **Ejecución del Proceso de Transición de estado de los teléfonos inteligentes**: Cada dispositivo en el espacio celular *C* recolecta información de sus vecinos para aplicar la función de transición y calcular su correspondiente estado su estado siguiente.
4. **Actualización de las variables de estado de los teléfonos inteligentes**: Actualización de los valores de cada teléfono inteligente de acuerdo a la dinámica para su uso en el siguiente paso de tiempo $t + 1$. Recolección de datos de cada teléfono inteligente para actualizar los valores de sus variables de estado y repetir el proceso incrementando el tiempo $t = t + 1$.

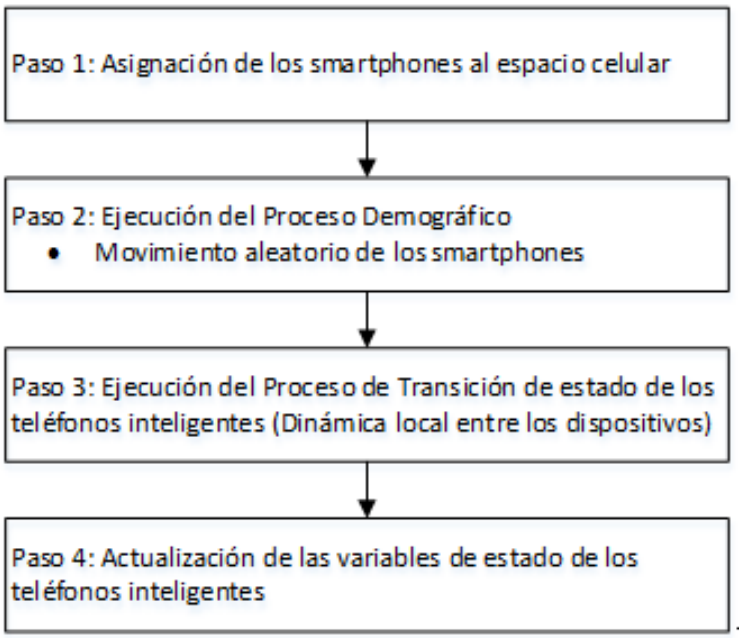


Fig. 3.8 - Diagrama de la Dinámica de Propagación del Gusano

3.2.1 Parámetros de Entrada

Para asignar valores a los parámetros que empleará el modelo, éstos se clasifican en parámetros generales y parámetros individuales.

3.2.1.1 Parámetros Globales

Los parámetros globales son aquellos que afectan a todo el sistema y no cambiaran durante el paso de tiempo de la simulación (detallados en la Tabla 3.2).

Probabilidad de Movimiento	P_{MOV}
Número de teléfonos inteligentes	N
Número inicial de Teléfonos inteligentes Infectados	$I(0)$
Tiempo de Latencia	T
Índice de Infección	β

Tabla 3.2 - Parámetros Globales de Entrada

3.2.1.2 Parámetros Individuales

Los parámetros individuales son aquellos que definen el comportamiento de cada uno de los teléfonos inteligentes e influyen directamente en la dinámica local con otros dispositivos. Los parámetros individuales considerados en este modelo son mostrados en la Tabla 3.3.

Probabilidad de aceptar la conexión Bluetooth	α
Probabilidad de que la antena Bluetooth este encendida	ε
Probabilidad de detección (Diagnosticar) del gusano	P_2
Probabilidad de remoción del gusano después del diagnostico	P_3

Tabla 3.3 - Parámetros Individuales

3.2.2 Reglas de Transición de Estado

Para describir el esparcimiento de malware vía Bluetooth en una población de teléfonos inteligentes se consideran las siguientes reglas que controlan la evolución del sistema:

Transición: Susceptible a Expuesto

Esta transformación de estado representa la situación en la que un teléfono inteligente "sano" entra en contacto con otro dispositivo infectado para dar inicio al proceso de infección. Para ilustrar lo anterior, supóngase que se tiene un teléfono inteligente en la posición (i, j), referido como u, con el estado actual de Susceptible ($\omega_{i,j}^{u}(t) = S$). El dispositivo u pasará al estado de Expuesto en el siguiente paso de tiempo ($\omega_{i,j}^{u}(t+1) = E$) si alguno de sus vecinos, denotado como v, cumple con

la probabilidad P_1 definida por la ecuación (3.2). Dado que el télefono inteligente u es afectado únicamente por otros teléfonos inteligentes en su vecindad, la probabilidad de que el teléfono inteligente u pase al estado expuesto se define como:

Fig. 3.9 - Transición de Susceptible a Expuesto

$$P_1 = \beta \frac{I_u(t)}{N_u} \tag{3.2}$$

Dónde N_u es el número total de vecinos de la célula u e $I_u(t)$ es el número de teléfonos infectados en la vecindad de u en el tiempo t.

Se asume que un teléfono inteligente Infectado siempre tiene su antena Bluetooth encendida, por lo tanto, para determinar si la comunicación entre un dispositivo infectado y un susceptible se da, es necesario que se cumplan dos condiciones: que el dispositivo al que se intenta contactar tenga la antena encendida y que acepte la conexión entrante. La función lógica empleada para modelar la condición que determinará si se establece un contacto entre la célula v y la célula u está dada por:

$$FL_1 = u_{BT} \wedge u_{AceptarCon\_v} \tag{3.3}$$

Donde u_{BT} representa un valor lógico en el que 1 indica que la antena del teléfono inteligente en la célula u está encendida con una probabilidad ε o se encuentra apagada con una probabilidad $1-\varepsilon$:

$$u_{BT} = \begin{cases} 1, \text{con probabilidad } \varepsilon \\ 0, \text{en caso contrario} \end{cases} \tag{3.4}$$

$u_{AceptarCon\_v}$ también representa un valor lógico, donde 1 indica que el teléfono inteligente en la célula u acepta la conexión entrante proveniente del teléfono inteligente en la célula v con probabilidad α o la rechaza con una probabilidad $1-\alpha$:

$$u_{AceptarCon\_v} \begin{cases} 1, \text{con probabilidad } \alpha \\ 0, \text{en caso contrario} \end{cases} \tag{3.5}$$

Por lo tanto, la transición de estado susceptible de un teléfono inteligente u al estado expuesto se define como:

$$\begin{gathered} ((rand() \leq P_1) \wedge FL_1 = 1) \\ \omega_{i,j}^{u}(t+1) = E \\ \neg((rand() \leq P_1) \wedge FL_1 = 1) \\ \omega_{i,j}^{u}(t+1) = S \end{gathered} \tag{3.6}$$

donde $rand() \in [0,1]$ denota un número aleatorio, el símbolo "∧" denota la operación lógica AND y el símbolo "¬" el operador lógico NOT.

Transición: Expuesto a Infectado o Expuesto a Interrumpido o Expuesto a Portador

Esta transformación de estado representa la situación en la que un teléfono inteligente Expuesto ya está en contacto con otro infectado y pueden darse tres posibles eventos: que el teléfono inteligente expuesto y el teléfono inteligente infectado se mantengan en el radio de transmisión *r* durante todo el tiempo de latencia hasta terminar el envío del gusano y que ambos dispositivos tengan el mismo sistema operativo, que el teléfono inteligente expuesto salga del radio de transmisión *r* del teléfono inteligente infectado y que el teléfono inteligente infectado complete la transmisión del gusano pero el teléfono inteligente receptor tenga un sistema operativo distinto al sistema objetivo del gusano. Para ilustrar lo anterior, supóngase que se tiene un teléfono inteligente en la posición (*i*, *j*), referido como u, con el estado actual de Expuesto ($\omega_{i,j}^{u}(t) = E$). El dispositivo u puede pasar a uno de los siguientes estados en el en tiempo $t+1$: Infectado $\omega_{i,j}^{u}(t+1) = I$, Interrumpido ($\omega_{i,j}^{u}(t+1) = I$), o Portador ($\omega_{i,j}^{u}(t+1) = P$), de acuerdo a las funciones lógicas mostradas en (3.7). En el caso particular de la transición al estado Infectado, u debe mantenerse en el radio de alcance del dispositivo infectado durante todo el tiempo de latencia T requerido para transmitir el gusano en su totalidad, de lo contrario, se asume que el teléfono expuesto salió del alcance de la antena Bluetooth del teléfono infectado. Este cálculo se evalúa de forma individual al emplear el atributo TII de cada agente que representa al dispositivo expuesto, de modo que el desplazamiento del tiempo obtenido de $TII + T$ da como resultado el tiempo en el que u cambia al estado de infectado.

Para ilustrar esta situación se supone que se tienen dos dispositivos expuestos denominados u y u' cuyos atributos son mostrados en la Tabla 3.4. Se observa que u pasó al estado Expuesto en $t = 10$ y u' en $t = 14$. Ambos teléfonos inteligentes se mantienen en el radio de alcance de los teléfonos inteligentes infectados que los hicieron pasar al estado Expuesto. La modelación de la transmisión del gusano en cuanto a tiempo se muestra en la Fig. 3.11 donde se asume un tiempo de latencia $T = 7$.

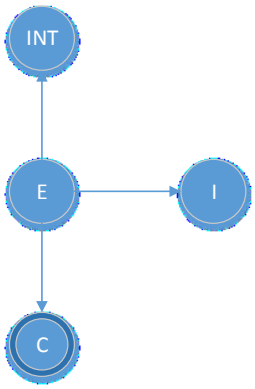


Fig. 3.10 - Transiciones del estado Expuesto

$$
\begin{aligned}
&(t < (TII + T)) \\
&\quad (v_{infectado} \in V_u) \\
&\quad\quad \omega_{i,j}^{u}(t+1) = E \\
&\quad (v_{infectado} \notin V_u) \\
&\quad\quad \omega_{i,j}^{u}(t+1) = INT \\
&(t \geq (TII + T)) \\
&\quad (v_{infectado} \in V_u \wedge u_{Tipo\ SO} = v_{Tipo\ SO}) \\
&\quad\quad \omega_{i,j}^{u}(t+1) = I \\
&\quad (v_{infectado} \in V_u \wedge u_{Tipo\ SO} \neq v_{Tipo\ SO}) \\
&\quad\quad \omega_{i,j}^{u}(t+1) = C
\end{aligned}
\qquad (3.7)
$$

donde $v_{infectado}$ denota a la célula vecina en estado infectado y V_u denota la vecindad de la célula u.

Parámetros de u		
	TipoSO	Android
	$\omega_{i,j}^{u}(t)$	Expuesto

Parámetros de u'		
	TipoSO	Android
	$\omega_{i,j}^{u}(t)$	Expuesto

	$\omega_{i,j}^{u}(t+1)$	
	Conectado con	$v_{infectado}$
	TII	10
	InfectPor	

	$\omega_{i,j}^{u}(t+1)$	
	Conectado con	$v_{infectado}{}'$
	TII	14
	InfectPor	

Tabla 3.4 - Ejemplificación Atributos de Agentes

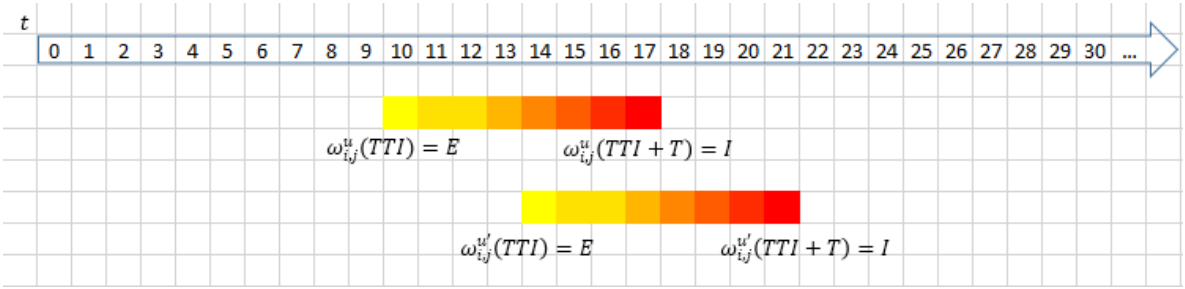


Fig. 3.11 - Línea de tiempo en la transición de Expuesto a Infectado suponiendo una T = 7

Transición: Interrumpido a Susceptible

Esta transformación de estado representa la situación en la que un teléfono inteligente expuesto estuvo en contacto con un dispositivo infectado pero alguno de los dos salió del radio de alcance de la antena Bluetooth antes de finalizar la transmisión del gusano, por lo tanto, se asume que la conexión fue interrumpida. En consecuencia, el teléfono expuesto no tiene una copia funcional del gusano por lo que no es afectado por éste, por tal motivo, el teléfono inteligente expuesto regresa nuevamente al estado de susceptible. Para ilustrar lo anterior, supóngase que se tiene un teléfono inteligente en la posición (*i*, *j*), referido como u, con el estado actual de Interrumpido ($\omega_{i,j}^{u}(t) = INT$), este pasará al estado de Susceptible al siguiente paso de tiempo de forma incondicional como se muestra en (3.8).

Fig. 3.12 - Transición de Interrumpido a Susceptible

$$\omega_{i,j}^{u}(t+1) = S \qquad (3.8)$$

Transición: Infectado a Diagnosticado

Esta transformación de estado representa el intento de detección de un programa anómalo en el sistema operativo del teléfono inteligente al emplear un software antivirus que ejecuta una revisión programada o actividad similar. En la práctica puede darse el caso en el que por obsolescencia del software antivirus no es posible detectar una firma de malware relativamente nueva. Para ilustrar lo anterior, supóngase que se tiene un teléfono inteligente en la posición (*i*, *j*), referido como u, con el estado actual de Infectado ($\omega_{i,j}^{u}(t) = I$), este pasa al estado diagnosticado con la probabilidad P_2 que indica que el malware de tipo gusano fue detectado como se muestra en (3.9).

Fig. 3.13 - Transición Infectado a Diagnosticado

$$(rand() \leq P_2) \quad \omega_{i,j}^{u}(t+1) = D \tag{3.9}$$

Transición: Diagnosticado a Infectado o Diagnosticado a Recuperado

Una vez que el gusano fue detectado en el sistema operativo del teléfono inteligente se intentará remover al aplicar la vacuna correspondiente. Al igual que en la transformación anterior, cabe la posibilidad de que el intento de remoción falle por falta de actualización del software antivirus haciendo que el teléfono inteligente continúe infectado. Para ilustrar lo anterior, supóngase que se tiene un teléfono inteligente en la posición (*i*, *j*), referido como u, con el estado actual de Diagnosticado ($\omega_{i,j}^{u}(t) = D$). El antivirus del dispositivo u intentará remover el gusano con una probabilidad P_3 y así pasar al estado siguiente de recuperado ($\omega_{i,j}^{u}(t+1) = R$) en el cual el dispositivo es inmune ante ese gusano. En caso contrario, el teléfono inteligente volverá al estado infectado al siguiente paso de tiempo ($\omega_{i,j}^{u}(t+1) = I$). Las condiciones lógicas que controlan esta transición son mostradas en (3.10).

Fig. 3.14 - Transiciones del estado Diagnosticado

$$(rand() \leq P_3) \quad \omega_{i,j}^{u}(t+1) = R$$
$$(rand() > P_3) \quad \omega_{i,j}^{u}(t+1) = I \tag{3.10}$$

En el capítulo 4 se detallaran los casos de estudio comprendidos en el presente trabajo junto con los resultados obtenidos en cada uno de ellos dependiendo de las variaciones en sus variables de entrada.

Capítulo 4: Casos de Estudio y Resultados

En este capítulo se presenta un análisis de los resultados generados al implementar el modelo los casos de estudio comprendidos en el presente trabajo de investigación, donde se emplea el modelo descrito en el capítulo anterior para generar simulaciones computacionales con la finalidad de validar su desempeño y la manera en cómo la variación de parámetros de entrada que reflejan situaciones reales afectan los resultados obtenidos.

4.1 Parámetros del Sistema (globales)

Para todos los resultados mostrados en este capítulo, se considera un espacio geográfico de 101×101 celdas, cada una de 1×1 m; es decir, se considera un área geográfica total de 10,201 m^2 que aproxima el tamaño de una manzana en una zona habitacional en México. Por simplicidad y para contar con una mejor apreciación visual del alcance de transmisión de la antena Bluetooth de los teléfonos inteligentes, se optó por una celda de estas dimensiones. El sistema evoluciona en pasos de tiempo de 1 segundo. Salvo que se especifique otro valor por así requerirse, los resultados mostrados se obtienen de simular 21,600 pasos de tiempo equivalentes a un total de 6 horas; este valor se consideró para representar el tiempo promedio en el que una persona permanece en el espacio geográfico simulado. Los resultados presentados se realizaron considerando una vecindad de Moore. Además, se considera una frontera asignada, de tal manera que para las celdas en la frontera, se suponen celdas virtuales como parte de su vecindad (aquellas fuera del espacio celular), las cuales están siempre están ocupadas por un teléfono en estado susceptible con la antena Bluetooth en estado de apagada. En la Tabla 4.1 se resumen los valores de los parámetros globales del modelo.

Duración de la Prueba	21,600 ticks (segundos)
Espacio Celular	101×101 = 10,302 m^2
Número de Simulaciones	20
Índice de Infección β	0.9
Tiempo de Latencia	25 segundos [37]
Tipo de Vecindad	Moore
Frontera	Asignada

Tabla 4.1 - Parámetros Globales de Cada Simulación

Los valores para el resto de los parámetros se indicarán en cada caso de estudio considerado para la evaluación del desempeño del modelo.

Para cada caso de estudio, se consideran 20 experimentos independientes, pero con las mismas condiciones iniciales (valores de los parámetros), cuyos resultados se promedian para mostrar el resultado, al menos que se indique lo contrario.

4.2 Resultados sin considerar movilidad

Inicialmente, con la finalidad de evaluar la racionalidad del modelo en su forma básica, se presentan resultados de simulación sin considerar el factor de movilidad de los teléfonos, es decir, con una probabilidad de movilidad de cero.

4.2.1 Relación entre Densidad y el tiempo de Propagación

Los gusanos para teléfonos inteligentes tienen el mismo comportamiento que los gusanos para estaciones de trabajo o computadoras personales fijas, su principal objetivo es auto-replicarse tan rápido como sea posible. La densidad de teléfonos es un factor muy importante. Debido a que se supone que el tamaño del área geográfica a simular es constante, como punto inicial se realizó un análisis de los efectos que produce el variar la densidad sobre la velocidad de propagación del gusano como una función del tiempo requerido para alcanzar una proporción de infección del 95% de la población total existente en el área geográfica bajo estudio.

Sea σ que denota la densidad de dispositivos, que se calcula como sigue:

$$\sigma = \frac{N}{L \times M} \qquad (4.1)$$

donde N corresponde al número total de teléfonos inteligentes desplegado en un espacio celular bidimensional C de $L \times M$ celdas, los cuales inicialmente se asignan en posiciones aleatorias.

Tipo de población	Homogénea
Densidad (Número de dispositivos)	10%, 20%, 30%, 40%, 50%, 60%, 70%, 80% y 90%
Número de infectados inicial *I(0)*	10% de la población total
Rango de la vecindad	1
Probabilidad de que la antena Bluetooth este encendida	1
Probabilidad de aceptación de la comunicación entre u y v	1
Probabilidad de detección del gusano	0

Probabilidad de remoción del gusano	0
Probabilidad de movimiento	0

Tabla 4.2 - Parámetros para el estudio de Velocidad de Propagación del Gusano

Así, se consideraron distintos valores de la densidad de teléfonos inteligentes al variar su valor entre el 10% y 90%. Para todos los valores de la densidad analizados, se usaron los valores de los parámetros que se muestran en la Tabla 4.2, los cuales se mantienen constantes durante la ejecución de todas las simulaciones. En la Fig. 4.1. se muestran los resultados obtenidos. Como se puede observar de esta figura, cuando la densidad de dispositivos es menor al 50%, la propagación del gusano no saturará el sistema, es decir, no se alcanza la proporción de infección establecida; esto se debe al corto rango de alcance de la antena Bluetooth modelada por el radio de la vecindad de Moore (1 m) y por lo tanto, a la distancia que existe entre los dispositivos susceptibles e infectados que supera el rango de alcance. Estos espacios vacíos entre los teléfonos forman una especie de cercos que desaceleran o incluso contienen la propagación del gusano. Sim embargo, para $\sigma \geq 50\%$, con el incremento de la densidad, la población de teléfonos inteligentes susceptibles e infectados aumenta también; entonces, la distancia entre los mismos (espacios vacíos) se reduce y la interacción entre los teléfonos se incrementa. Como consecuencia, un teléfono inteligente en estado susceptible (S) puede verse amenazado por más dispositivos infectados aumentando la probabilidad de que pase al estado expuesto (E) y por lo tanto, la población total se sature más rápido por la infección del gusano conforme la densidad se incrementa. Es por ello que el tiempo de infección se reduce a medida que la densidad de teléfonos se incrementa debido a que la cantidad de contactos efectivos para la infección es mayor.

Se establece un criterio de paro adicional para este caso de estudio para que la simulación se detenga cuando el número de dispositivos infectados alcance el 95% o más. Los resultados de la simulación son mostrados en la Fig. 4.1.

Como se puede observar en la gráfica anterior, cuando la densidad de dispositivos es menor al 50%, el gusano no logra saturar el sistema al infectar a la población de teléfonos inteligentes susceptibles. Esto se debe al corto rango de alcance de la antena Bluetooth modelada por el radio de la vecindad de Moore y a la distancia que hay entre los dispositivos susceptibles e infectados. Estos huecos forman cercos que desaceleran o incluso contienen la propagación del gusano. A medida que los espacios se reducen conforme la población de teléfonos inteligentes susceptibles e infectados aumenta, un teléfono inteligente susceptible puede verse amenazado por más dispositivos infectados aumentando la probabilidad de que pase al estado expuesto. Asimismo, se observa que las densidades superiores al 50% favorecen a la propagación del gusano.

Cuando la densidad de dispositivos es del 90% se observa que el gusano tiene las condiciones espaciales para lograr infectar al 95% de la población de dispositivos al paso de 150 segundos en promedio. El tiempo de infección se reduce a medida que la densidad aumenta haciendo que la cantidad de contactos efectivos para la infección sea mayor.

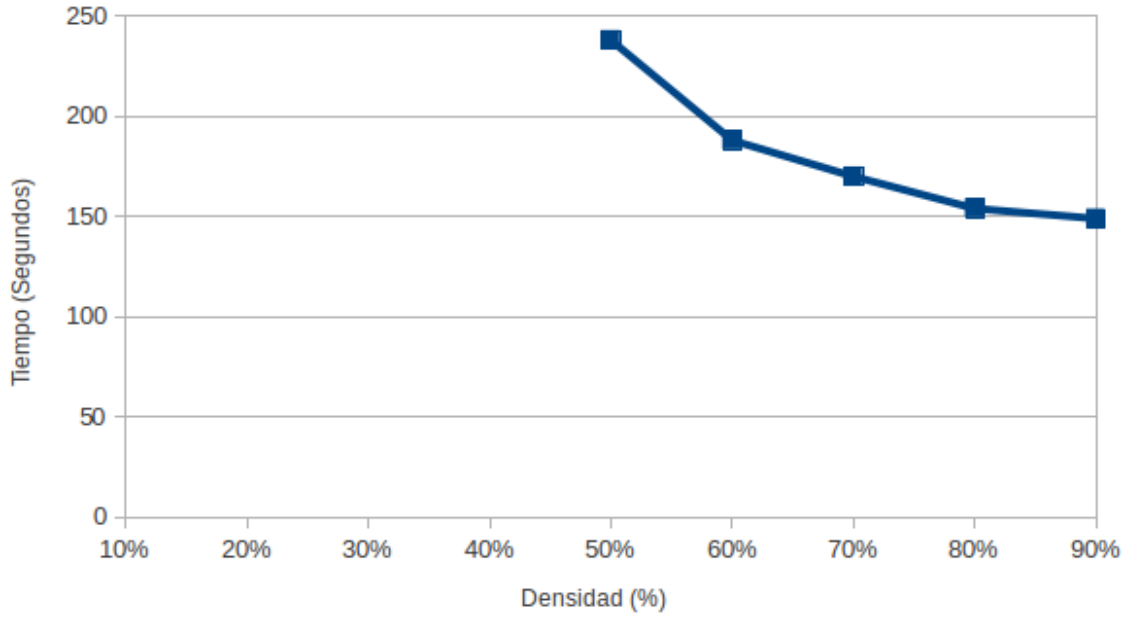


Fig. 4.1 - Relación entre la Densidad de teléfonos y el tiempo de Propagación de la infección (saturación)

Con base en los resultados obtenidos mostrados en la Fig. 4.1, en lo siguiente sólo se consideran valores para la densidad mayores o iguales al 50%.

Por otra parte, en la Fig. 4.2 se muestra la evolución de la infección del gusano cada segundo hasta alcanzar la proporción de infección máxima posible para diferentes valores de la densidad σ. Como puede notarse de esta figura, el tiempo promedio en el que el sistema alcanza el 95% de dispositivos infectados es de 230 segundos aproximadamente, a excepción del caso donde $\sigma = 50\%$ donde el máximo definido para esta prueba fue alcanzado después de 284 segundos, ya que las interacciones entre los teléfonos no es suficiente para permitir una propagación de infección rápida.

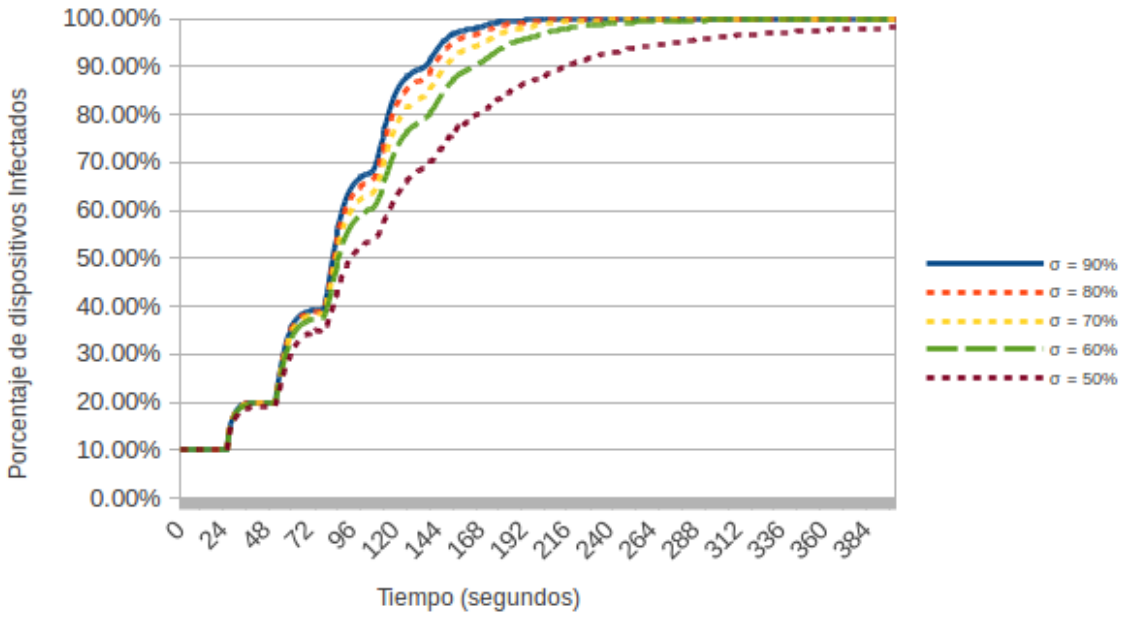


Fig. 4.2 - Comparación de la evolución de la infección del gusano en función del tempo para diferentes valores de la densidad promedio de teléfonos inteligentes

Es interesante notar que el tiempo en el que se inicia la propagación del contagio, es decir, donde el porcentaje de infectados iniciales se empieza a incrementar, es independiente de la densidad inicial, casi es el mismo para todas las densidades y la curva de propagación es semejante para todas las densidades hasta aproximadamente el segundo 60. Después de este tiempo, la curva de la propagación del gusano crece más rápido en el tiempo conforme el valor de la densidad se incrementa, como consecuencia del incremento natural de la interacción entre los teléfonos que propicia el contacto por alcance para transmitir la infección.

4.2.2 Variación del Estado de la Antena Bluetooth

En las pruebas anteriores se observó una rápida propagación del gusano donde al no contar con algún mecanismo de prevención en la población, el gusano se propagaba libremente a menos que por cuestiones de densidad y distribución de los teléfonos inteligentes el alcance de la antena Bluetooth no fuera suficiente para contactar a un dispositivo fuera de su radio. Sin embargo, uno de los factores importantes para que el contagio del gusano a través de Bluetooth suceda es que la antena del teléfono que se contacta esté encendida. Así, se estudió el impacto que tiene la probabilidad de que la antena Bluetooth se encuentre encendida, *BT*, sobre la propagación del gusano, variando su valor entre 0.2 y 0.9 con incrementos de 0.1 y para diferentes valores de la densidad. Cabe mencionar que no se considera ningún mecanismo de seguridad que frene la propagación del modelo, que más adelante se consideran. Además, sin pérdida de generalidad, se

supone que la probabilidad de aceptación de la comunicación siempre es 1. Se considera un tiempo de simulación de 21,600 pasos de tiempo. Los parámetros usados se resumen en la Tabla 4.3.

Tipo de población	Homogénea
Densidad (Número de dispositivos)	50%, 60%, 70%, 80%, 90%
Número de infectados inicial *I(0)*	10% de la población total
Rango de la vecindad	1
Probabilidad de que la antena Bluetooth este encendida	0.9, 0.8, 0.7, 0.6, 0.7 0.6, 0.5, 0.4, 0.3 y 0.2
Probabilidad de aceptación de la comunicación entre u y v	1
Probabilidad de detección del gusano	0
Probabilidad de remoción del gusano	0
Probabilidad de movimiento	0

Tabla 4.3 - Parámetros para el estudio de Propagación del Gusano basado en el estado de la antena Bluetooth de cada dispositivo

La Fig. 4.3 se muestra la curva de infección (teléfonos infectados) como función de la probabilidad BT para diferentes valores de la densidad. Nótese de esta figura que a medida que la probabilidad BT de que la antena Bluetooth de los dispositivos se encuentre encendida es menor, el porcentaje total de dispositivos infectados obtenido al finalizar la prueba también es menor. Los resultados promedio obtenidos de todas las simulaciones y mostrados en la misma figura, sugieren que la proporción de infectados final es proporcional al valor de BT, independientemente de la densidad, como es de esperarse al no haber mecanismo alguno que frene la propagación. Con la finalidad de analizar mejor el comportamiento obtenido, en las Fig. 4.4 a la Fig. 4.8 se muestran las curvas de infección con respecto al tiempo para diferentes valores de la probabilidad BT correspondientes a densidades de 50%, 60%, 70%, 80% y 90%, respectivamente. Como puede notarse de estas figuras, la velocidad de propagación del gusano es mayor a medida que σ se incrementa.

Considerando la ecuación (3.3) descrita en el capítulo anterior, la función lógica que determina si el contacto entre el teléfono inteligente u y el teléfono inteligente v se establece o no, requiere que una condición *AND* sea verdadera, éste planteamiento también involucra a la probabilidad α empleada en la función de casos (3.5). Así, el comportamiento será semejante al mostrado en las Fig. 4.4 a la Fig. 4.8, si se varía sólo la probabilidad de aceptación de la conexión entrante α.

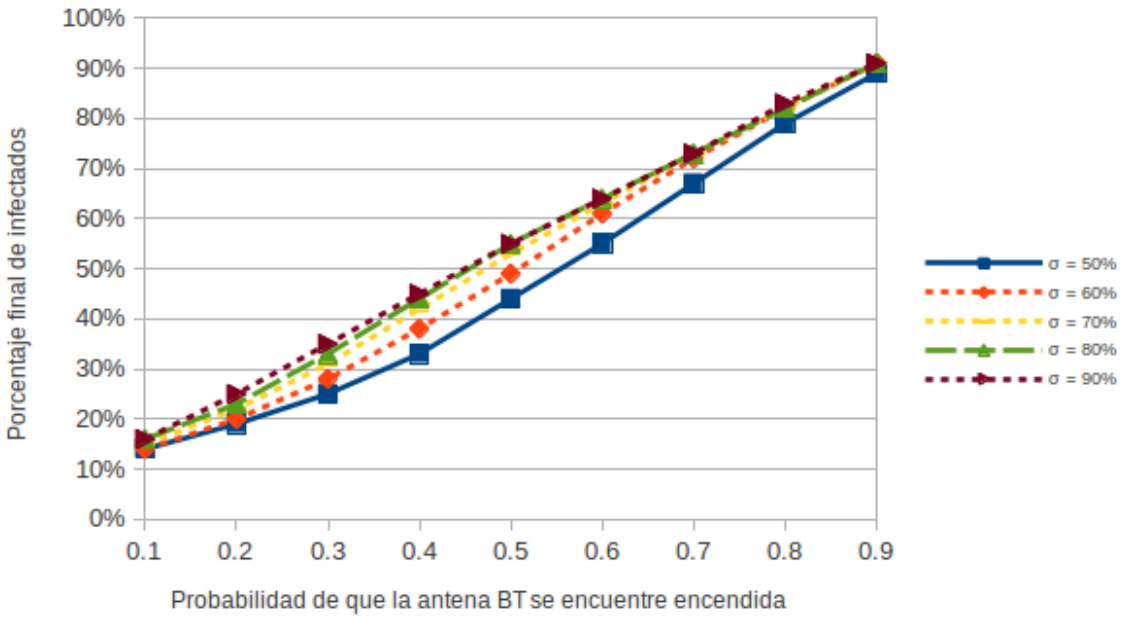


Fig. 4.3 - Porcentaje final de infectados con respecto a la probabilidad BT para diferentes valores de la densidad, donde BT corresponde a la probabilidad de que la antena Bluetooth de un dispositivo se encuentre encendida y σ *a la densidad*

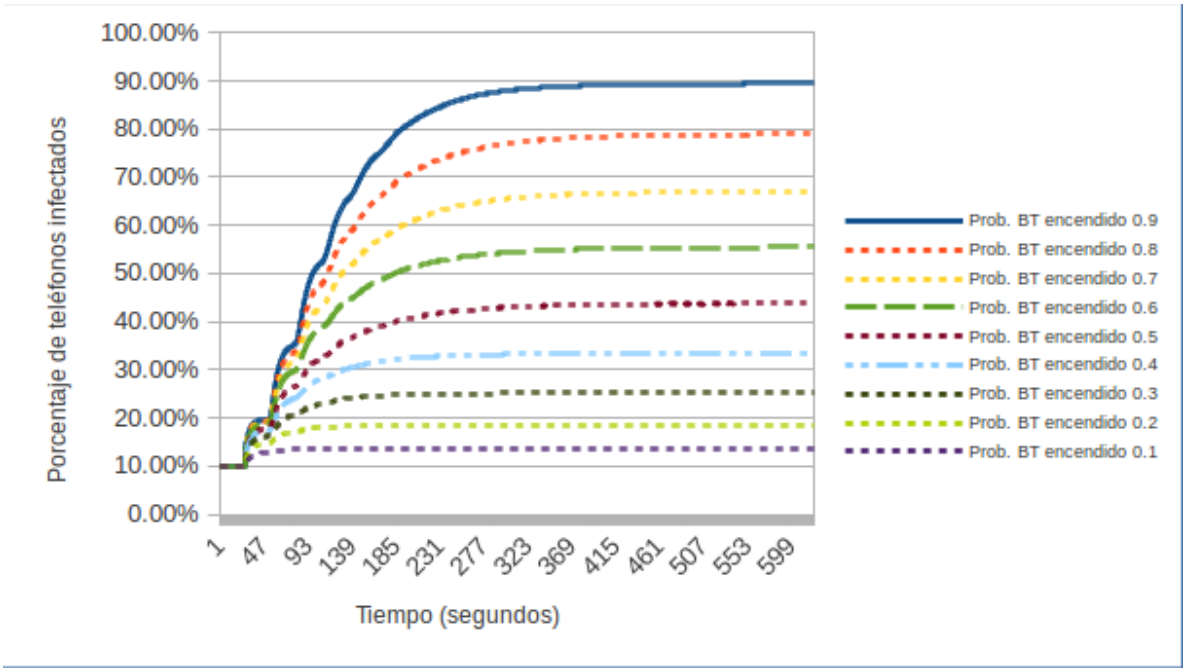


Fig. 4.4 - Curvas de infección del gusano en el tiempo para una densidad σ *del 50% y diferentes valores de BT, donde BT corresponde a la probabilidad de que la antena Bluetooth de un dispositivo se encuentre encendida.*

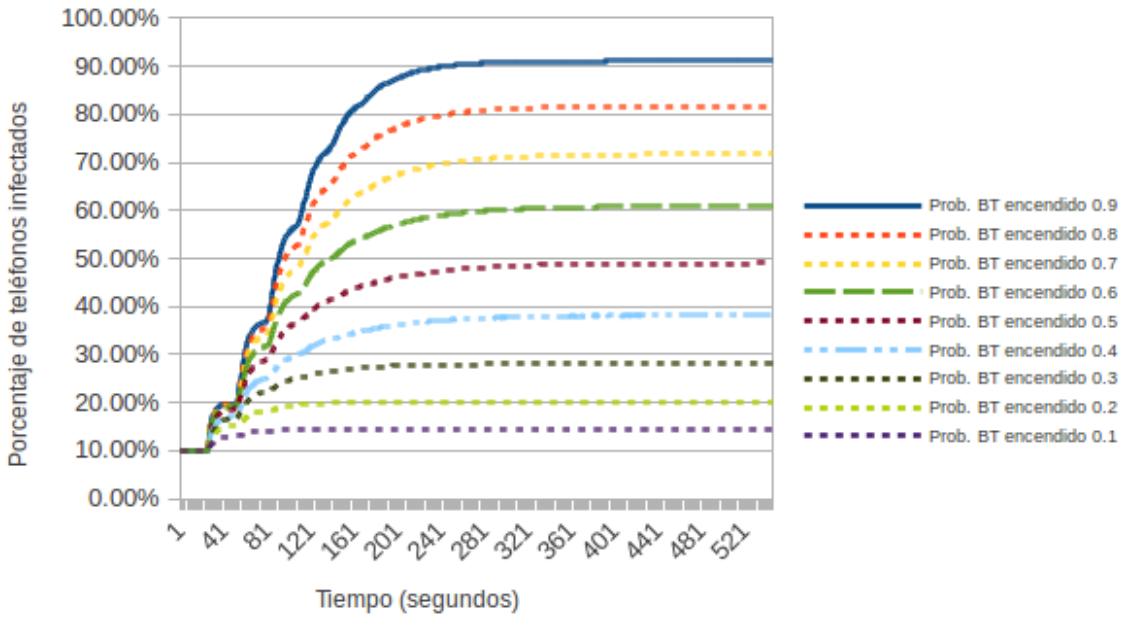


Fig. 4.5 - Curvas de infección del gusano en el tiempo para una densidad σ del 60% y diferentes valores de BT, donde BT corresponde a la probabilidad de que la antena Bluetooth de un dispositivo se encuentre encendida.

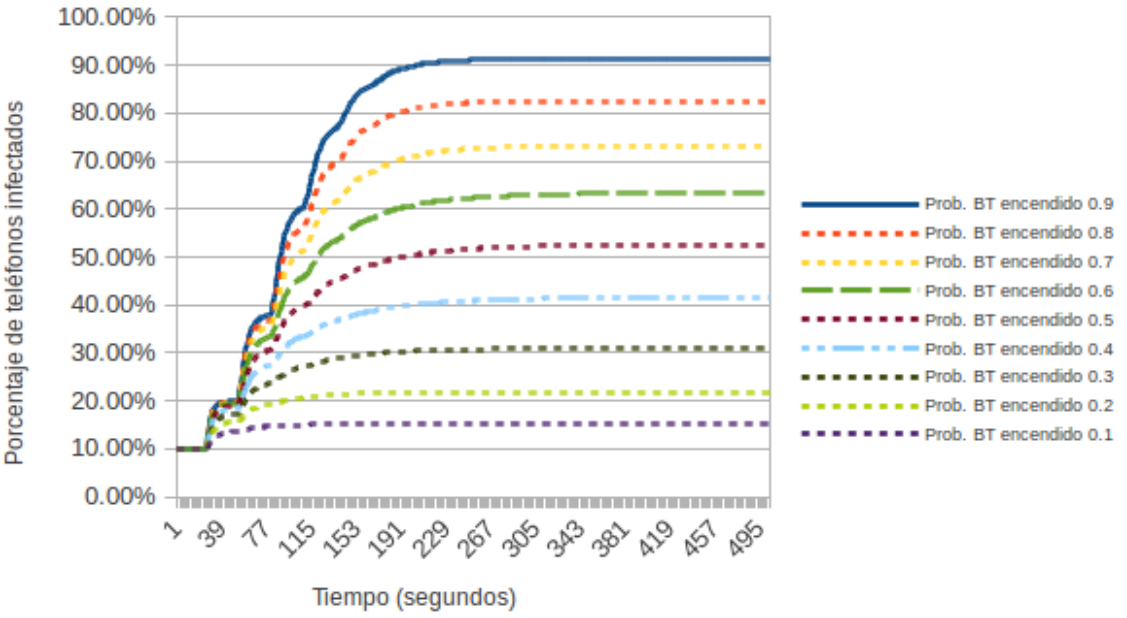


Fig. 4.6 - Curvas de infección del gusano en el tiempo para una densidad σ del 70% y diferentes valores de BT, donde BT corresponde a la probabilidad de que la antena Bluetooth de un dispositivo se encuentre encendida.

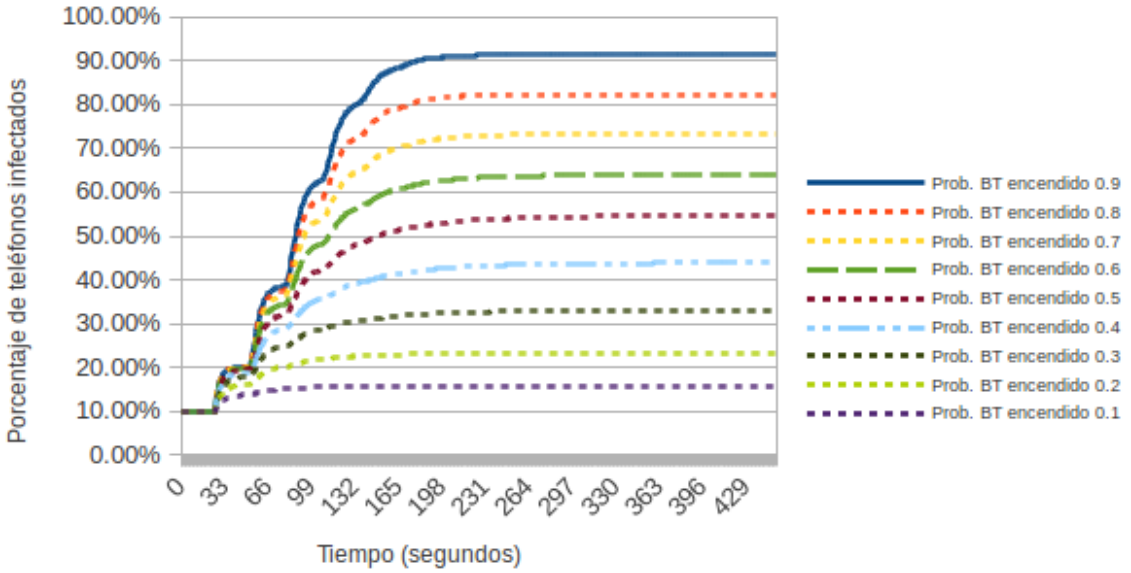


Fig. 4.7 - Curvas de infección del gusano en el tiempo para una densidad σ del 80% y diferentes valores de BT, donde BT corresponde a la probabilidad de que la antena Bluetooth de un dispositivo se encuentre encendida.

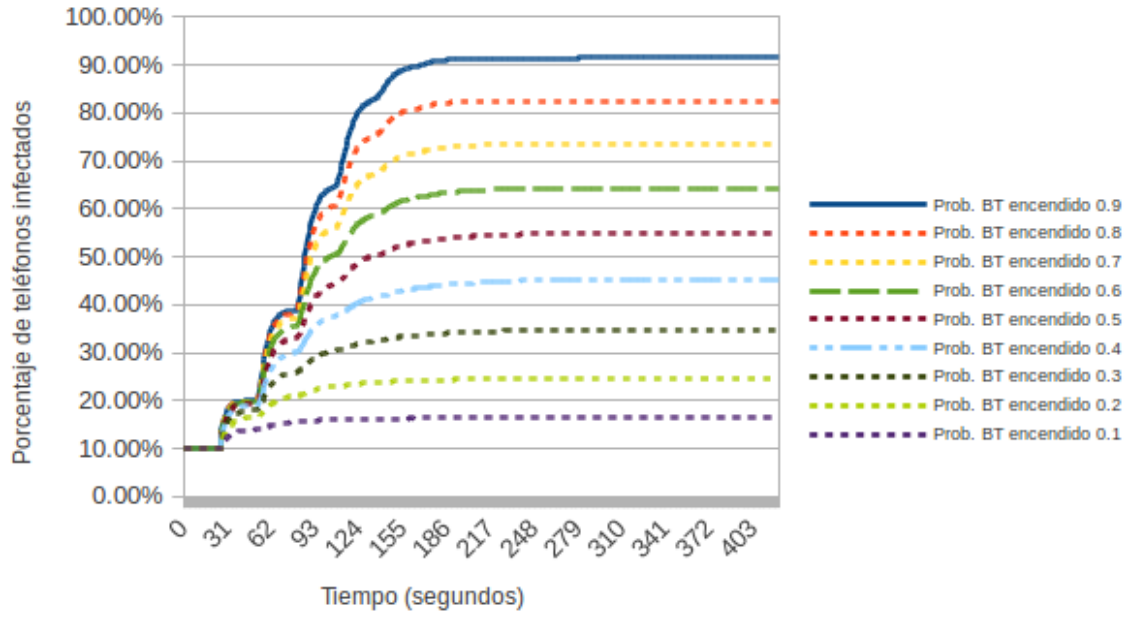


Fig. 4.8 - Curvas de infección del gusano en el tiempo para una densidad σ del 90% y diferentes valores de BT, donde BT corresponde a la probabilidad de que la antena Bluetooth de un dispositivo se encuentre encendida.

4.2.3 Variación del tipo de Población

Por otra parte, dada la gran demanda de teléfonos inteligentes existen varios fabricantes los cuales, entre otras cosas, generan distintos tipos de sistemas operativos para sus dispositivos con características particulares. Por ejemplo, en el caso de Apple, su sistema operativo sólo puede ser instalado en dispositivos de esta misma marca, por el contrario, el sistema operativo Android puede ser instalado en dispositivos fabricados por distintas compañías, lo cual le da una mayor porción del mercado (14.8% y 84.1% respectivamente hasta el primer trimestre del 2016 [38]). Al igual que en las epidemias biológicas, las diferencias en las características de la población (número total de dispositivos desplegados en un espacio geográfico dado) de teléfonos inteligentes afectarán la dinámica de propagación del gusano y estarán directamente relacionadas con la cantidad de dispositivos que pasarán al estado de Portador. Dicho estado representa una condición en la que un dispositivo recibió una copia útil del gusano pero al tener un sistema operativo objetivo diferente al teléfono que lo contactó, el malware no entrará en funcionamiento.

Así, también se analizó el desempeño del modelo cuando se considera una población heterogénea, es decir, que 84% de los teléfonos tienen sistema operativo Android, 15% tienen iOS y el resto tienen otro tipo de sistema operativo (ver la Fig. 4.9). Particularmente, se analiza la evolución de la propagación del gusano en el espacio y el tiempo para distintos valores de la densidad. Para ello se utilizan los valores de los parámetros especificados en la Tabla 4.4.

Tipo de Población	Heterogénea
Sistema operativo objetivo del gusano	Android
Densidad (Número de dispositivos)	50%, 60%, 70%, 80%, 90%
Rango de la Antena Bluetooth	1
Número inicial de Infectados $I(0)$	10% de la población total
Probabilidad de Aceptación de conexión Bluetooth	1
Probabilidad de detección del Gusano P_2	0
Probabilidad de Remoción del Gusano P_3	0
Probabilidad de movimiento	0

Tabla 4.4 - Parámetros de prueba para Población Heterogénea

En la Fig. 4.10 y Fig. 4.11, se muestra la evolución en el tiempo del porcentaje de infectados y portadores de la población total, respectivamente, para diferentes valores de la densidad de los teléfonos inteligentes. Como puede notarse de la Fig. 4.10, independientemente de la densidad, el porcentaje de teléfonos en un estado infectado se incrementa con el paso del tiempo hasta alcanzar un máximo equivalente al porcentaje total de los teléfonos de la población con sistema operativo Android considerado (84% de la población). Este comportamiento se debe a que en las simulaciones realizadas no se considera algún mecanismo de protección (antivirus, antena apagada, etc.) que limite la propagación del gusano, por lo que el gusano se puede propagar en el tiempo al total de

la población de teléfonos inteligentes, excepto a aquellos con sistema operativo distinto a Android (16% de la población, ver la Fig. 4.11); que aunque sí pueden ser alcanzados por el gusano pasarán a un estado de portador), ya que se considera que el gusano sólo es capaz de infectar a dispositivos con sistema operativo Android.

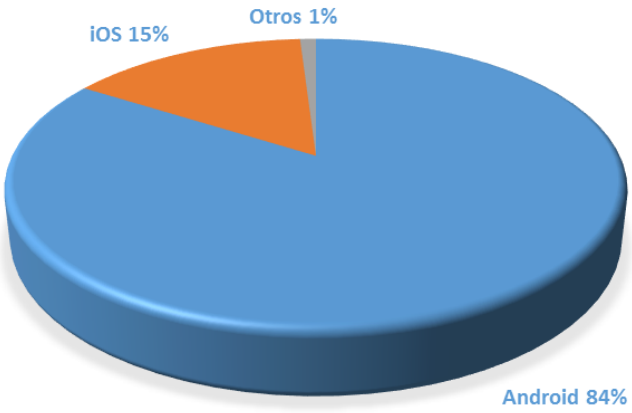


Fig. 4.9 - Porción de mercado de Sistemas Operativos para Teléfonos inteligentes

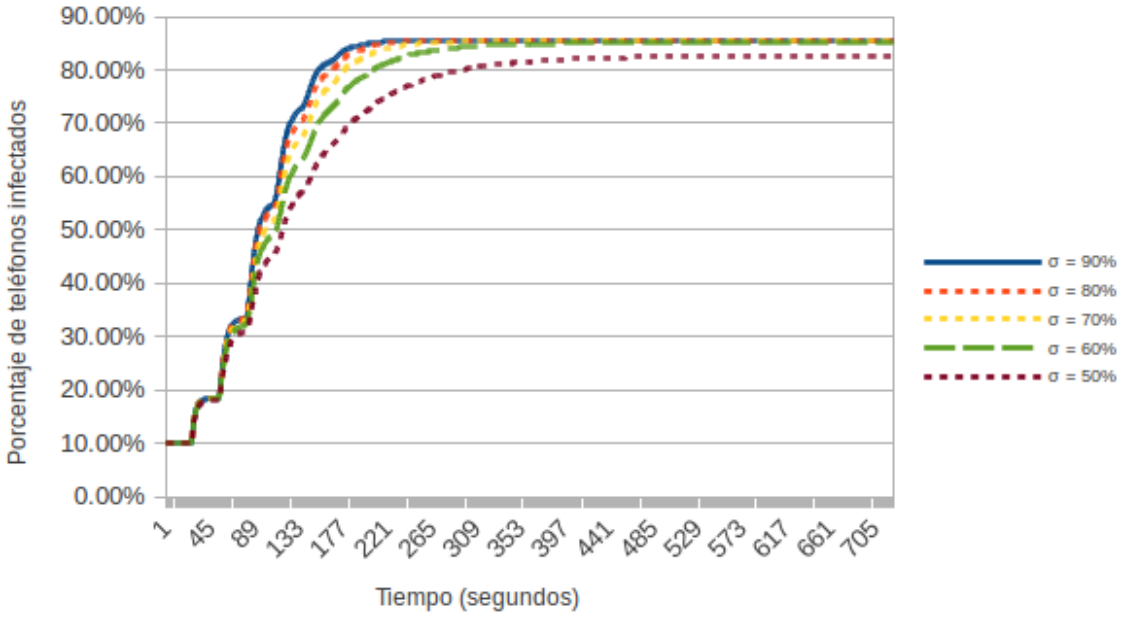


Fig. 4.10 - Comparación de la curva de infección del gusano en función del tiempo

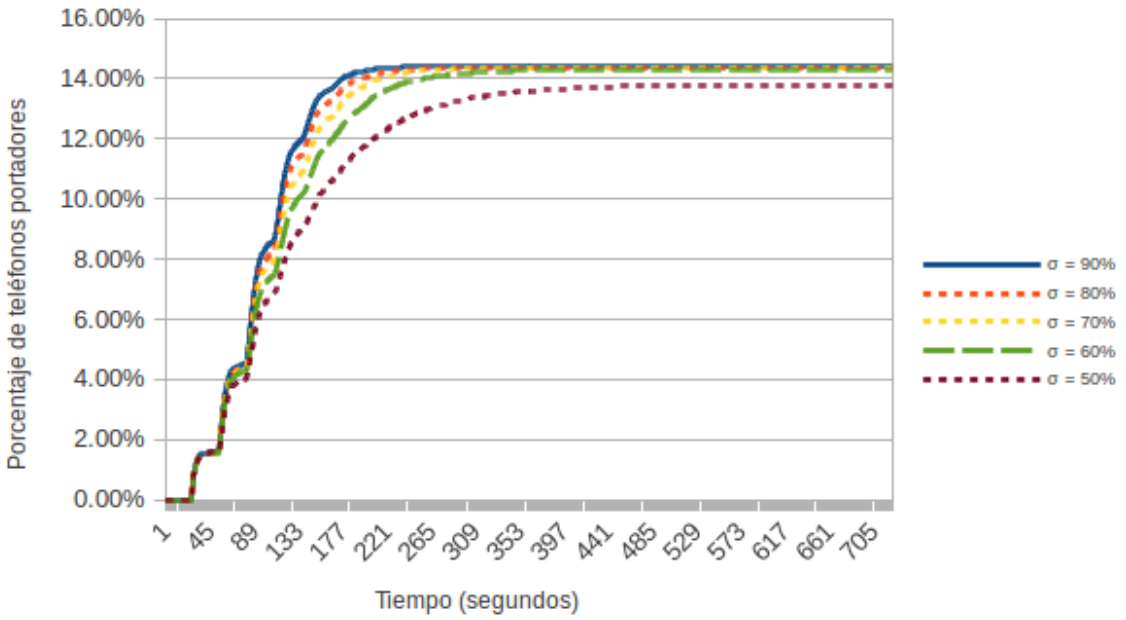


Fig. 4.11 - Comparación de la curva de generación de portadores del gusano en función del tiempo

En las Fig. 4.12 y Fig. 4.13, se resumen los resultados de propagación del gusano mostrados previamente para una población de teléfonos homogénea (sección 4.2.1) y heterogénea, respectivamente. Independientemente de la población considerada, cómo era de esperarse, la proporción de dispositivos afectados por el gusano en ambas casos es prácticamente la misma. Estos resultados indican que la dinámica definida para el modelo funciona como se esperaba y su dinámica es coherente.

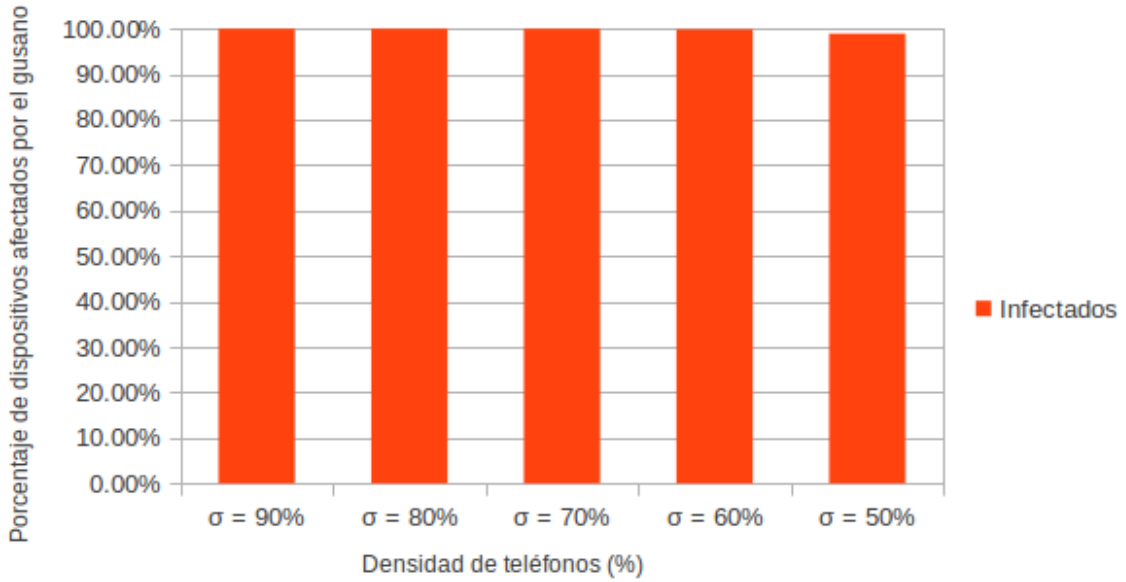


Fig. 4.12 - Porcentaje de dispositivos afectados por el gusano en una población homogénea

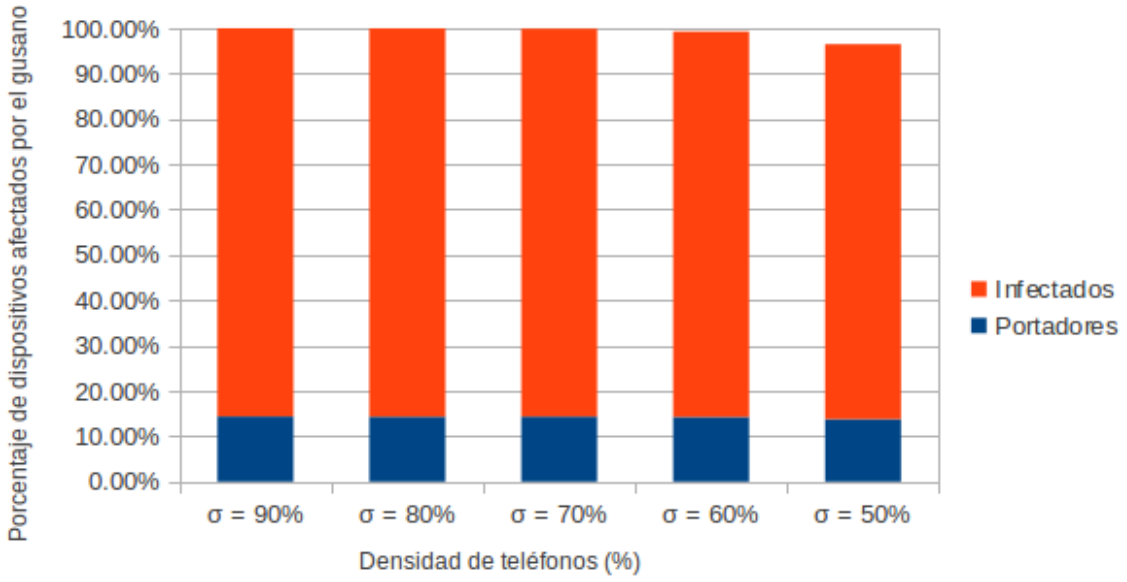


Fig. 4.13 - Porcentaje de dispositivos afectados por el gusano en una población heterogénea

4.2.4 Variación del Factor de recuperación y detección del gusano

Unos de los parámetros claves del modelo para la evolución de la propagación y su velocidad son la probabilidad de que un teléfono pase de un estado *Infectado* a uno *Diagnosticado* (P_2) y la probabilidad de que un teléfono pase de un estado *Diagnosticado* a un estado *Recuperado* (P_3). Así su impacto en el desempeño de la propagación es de gran importancia. Para llevar a cabo este análisis, se consideró que la todos los teléfonos siempre tienen la antena encendida y siempre aceptan una petición de conexión a través de Bluetooth. Los valores de los parámetros se resumen en la Tabla 4.5. Cabe mencionar que por simplicidad, la densidad de teléfonos es constante en el tiempo, sólo se cambian los estados de los teléfonos en el tiempo. Además, se supone que P_2=P_3, es decir, que la probabilidad de pasar de *Infectado a Diagnosticado* es la misma que de *Diagnosticado* a *Recuperado.*

Tipo de Población	Homogénea
Densidad (Número de dispositivos)	50%, 60%, 70%, 80%, 90%
Rango de la Antena Bluetooth	1
Número inicial de Infectados $I(0)$	10% de la población total
Probabilidad de Aceptación de conexión Bluetooth	1
Probabilidad de detección del Gusano P_2	0.10, 0.20, 0.30, 0.40, 0.50, 0.60, 0.70, 0.80, 0.90
Probabilidad de Remoción del Gusano P_3	
Probabilidad de movimiento	0

Tabla 4.5 - Parámetros de prueba para la variación del factor de recuperación y detección del gusano

En las figuras Fig. 4.14, Fig. 4.15 y Fig. 4.16 se muestra la evolución en el tiempo del número de dispositivos en los diferentes estados para P_2 igual a 0.1, 0.5 y 0.8, respectivamente, y $P_2 = P_3$, para una densidad del 80% y considerando teléfonos homogéneos. Como puede observarse de las figuras, al inicio la mayoría de los teléfonos se encuentran en estado susceptible, con el incremento del tiempo el número de teléfonos susceptibles se decrementa conforme el número de recuperados se incrementa. Nótese que a medida que el valor de la probabilidad de diagnóstico y recuperación es mayor, el tiempo requerido para que el sistema se estabilice disminuye, debido a que una cantidad mayor de dispositivos infectados se recupera cada instante de tiempo. Además, como también puede observarse de las figuras, el número de infectados máximo es menor conforme la probabilidad de diagnóstico (recuperación) es mayor; debido a que se frena la propagación de la infección por los mecanismos de detección. Es importante mencionar que no se considera un factor de renovación de la población, es decir, que un porcentaje de la población que se recupera pase nuevamente a un estado susceptible, por lo que la infección después de que logra alcanzar un máximo se decrementa con el tiempo

A medida que la probabilidad de diagnóstico y recuperación aumentan, el tiempo requerido para que el sistema se estabilice disminuye debido a que una cantidad mayor de dispositivos infectados es recuperada al mismo tiempo frenando la propagación del gusano.

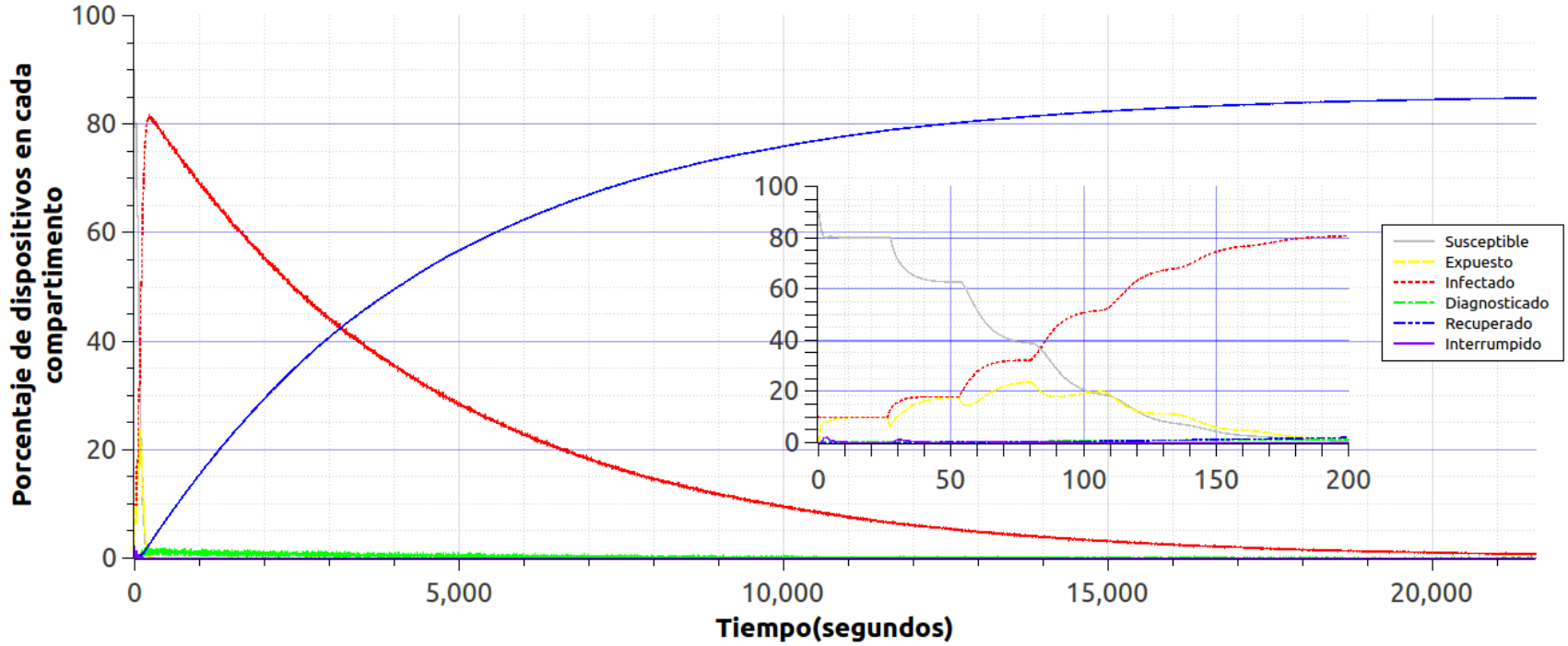


Fig. 4.14 - Evolución de los compartimentos para una densidad σ = 80% con probabilidad de diagnóstico P_2 = 0.1 y probabilidad de remoción del gusano P_3 = 0.1. La gráfica interior representa a la misma gráfica externa pero sólo para los primeros 200 segundos de evolución

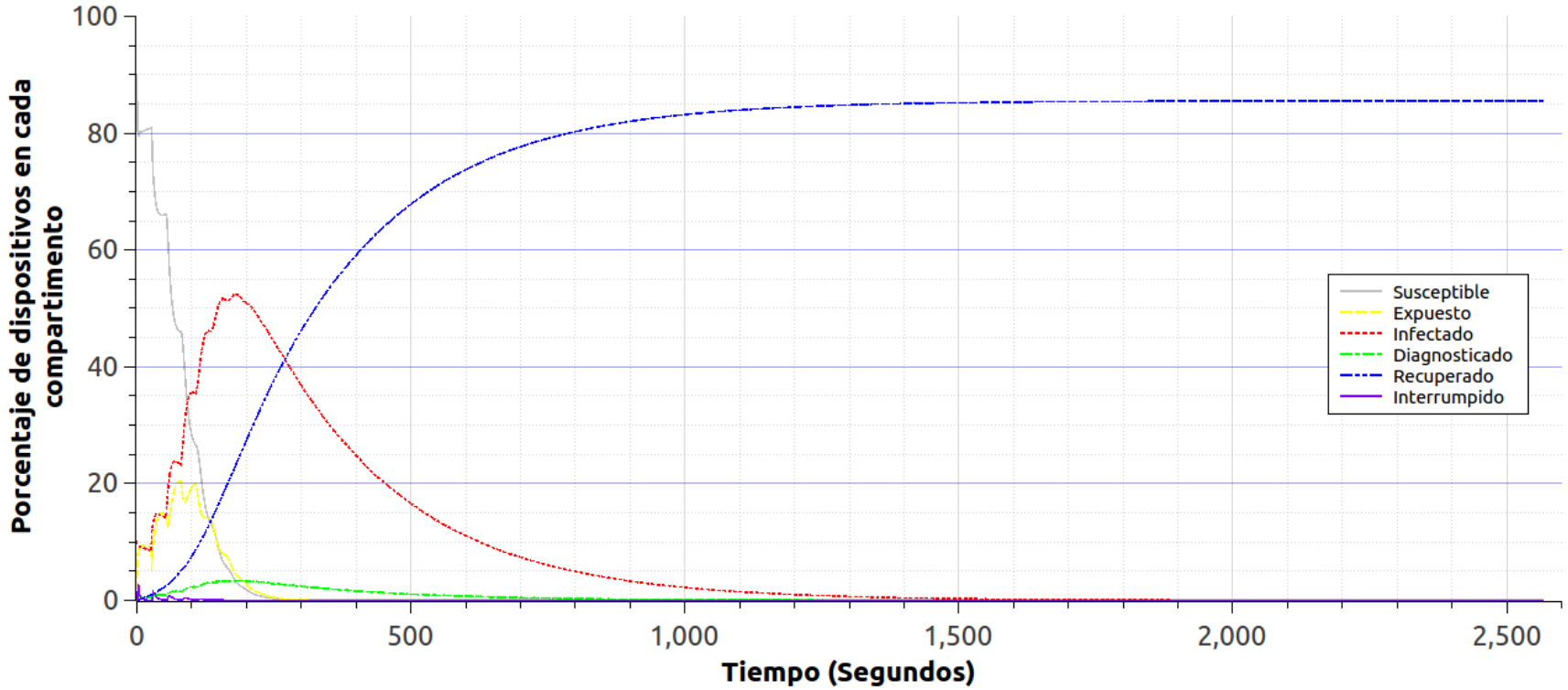


Fig. 4.15 - Evolución de los compartimentos para una densidad σ = 80% con probabilidad de diagnóstico $P_2 = 0.6$ y probabilidad de remoción del gusano $P_3 = 0.6$

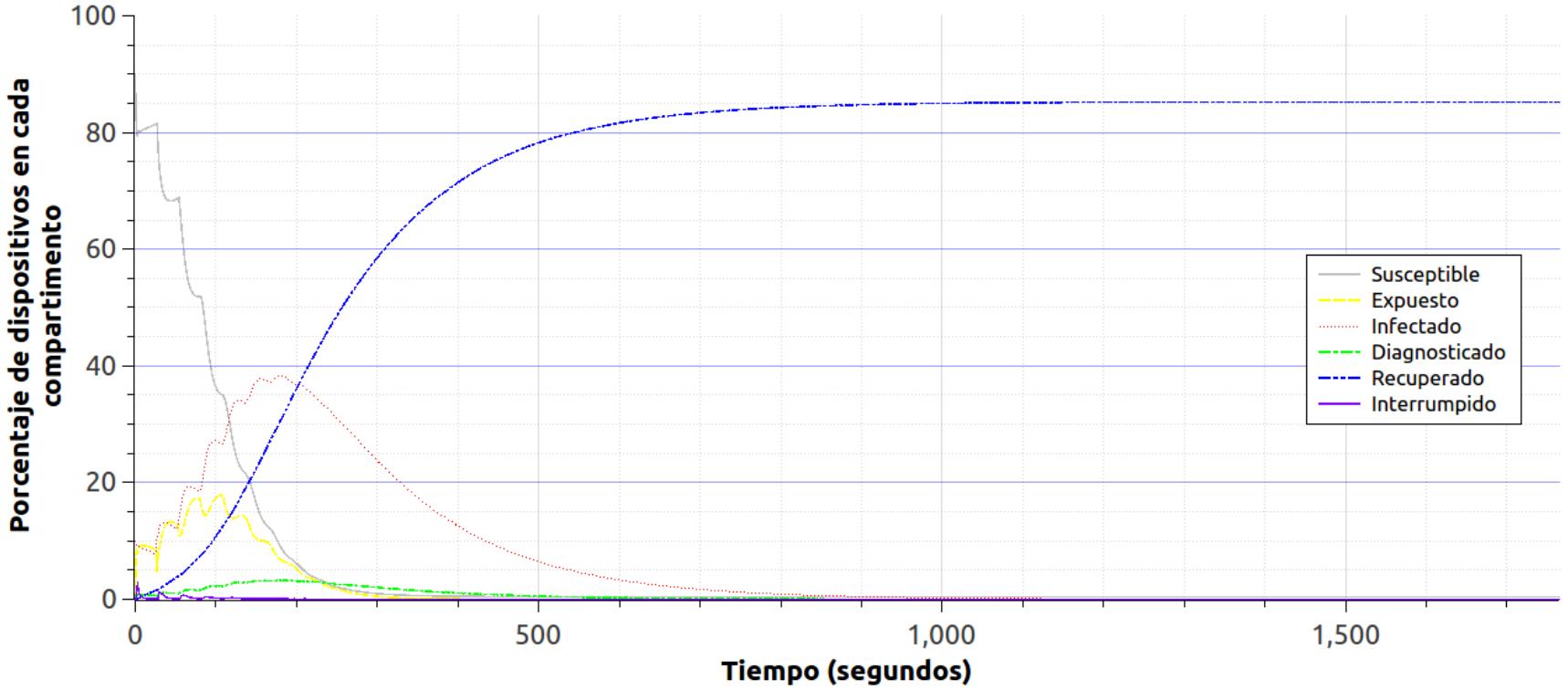


Fig. 4.16 - Evolución de los compartimentos para una densidad σ = 90% con probabilidad de diagnóstico $P_2 = 0.8$ y probabilidad de remoción del gusano $P_3 = 0.8$

4.2.5 Variación del Alcance de la Antena Bluetooth

Por otra parte, las conexiones Bluetooth no están limitadas a conexiones de corto alcance, de acuerdo con [3], existen tres clases de antenas Bluetooth en la Tabla 4.6; las cuales se diferencian por su rango de alcance operacional. La efectividad del rango de alcance varía en función de las condiciones de propagación, variación de la producción de las antenas, configuración del dispositivo y condiciones de la batería.

Clase	Radio de alcance
Clase 3	1 metro
Clase 2	10 metros
Clase 1	100 metros

Tabla 4.6 - Clasificación de las antenas Bluetooth según su rango de alcance

Para efectos de este experimento, se asume que cada antena simulada transmite a la máxima capacidad que le permite su clase. Las condiciones de la batería que pudieran afectar el desempeño de las antenas no son consideradas. Para la ejecución de las simulaciones se consideran los parámetros mostrados en la Tabla 4.7 dónde lo único que varía es el alcance de la antena.

Tipo de Población	Homogénea
Densidad (Número de dispositivos)	50%, 60%, 70%, 80%, 90%
Rango de la Antena Bluetooth	1, 10, 100
Número inicial de Infectados $I(0)$	10% de la población total
Probabilidad de Aceptación de conexión Bluetooth	1
Probabilidad de detección del Gusano P_2	0
Probabilidad de Remoción del Gusano P_3	0
Probabilidad de movimiento	0

Tabla 4.7 - Parámetros de prueba para variación del alcance de la antena Bluetooth

Los resultados obtenidos en cada prueba son organizados para establecer un comparativo visual del desempeño de cada clase para cada densidad (ver Fig. 4.17 a Fig. 4.21). En todos los casos se observa que el comportamiento de la propagación cuando se emplean radios *r = 1* y *r = 10* es semejante durante los primeros pasos de tiempo, de igual manera, ésta similitud es mayor cuando la densidad de la población de teléfonos inteligentes es baja. Para todos los casos, se observa que para toda $r > 1$, la propagación del gusano sólo puede afectar como máximo al 86% de la población total de teléfonos inteligentes. Esto se debe a que en esta configuración, cada dispositivo tiene una vecindad mucho más grande, lo cual genera que estas se traslapen entre ellas sobreestimando la propagación, ya que el AC funciona de manera síncrona, cada agente que representa un teléfono inteligente aplica sus reglas de transición local de manera simultánea. En el caso concreto de los teléfonos inteligentes en estado infectado, éstos generarán un listado de teléfonos inteligentes susceptibles

que pueden contactar dentro de su rango *r*, no obstante, una de las condiciones descritas en la presentación del modelo, restringe a que sólo un dispositivo infectado puede establecer una conexión con un dispositivo susceptible (contacto efectivo) en el tiempo *t*. Suponiendo el caso peor, *x* números de teléfonos inteligentes infectados generan su propio listado de teléfonos inteligentes susceptibles y en dichos listados se encuentra el teléfono inteligente *u*, durante la fase del cálculo de las variables de cada teléfono inteligente para el tiempo $t + 1$, y también suponiendo que la probabilidad de contagio sea 1 (evento seguro) para todos, el primer dispositivo infectado que establezca la conexión con el dispositivo *u* hará que $x - 1$ dispositivos restantes, automáticamente pierdan ese intento de contagio. Por lo tanto, a mayor rango de transmisión r, mayor es la probabilidad de traslape y por consecuencia de *congestionar* la red.

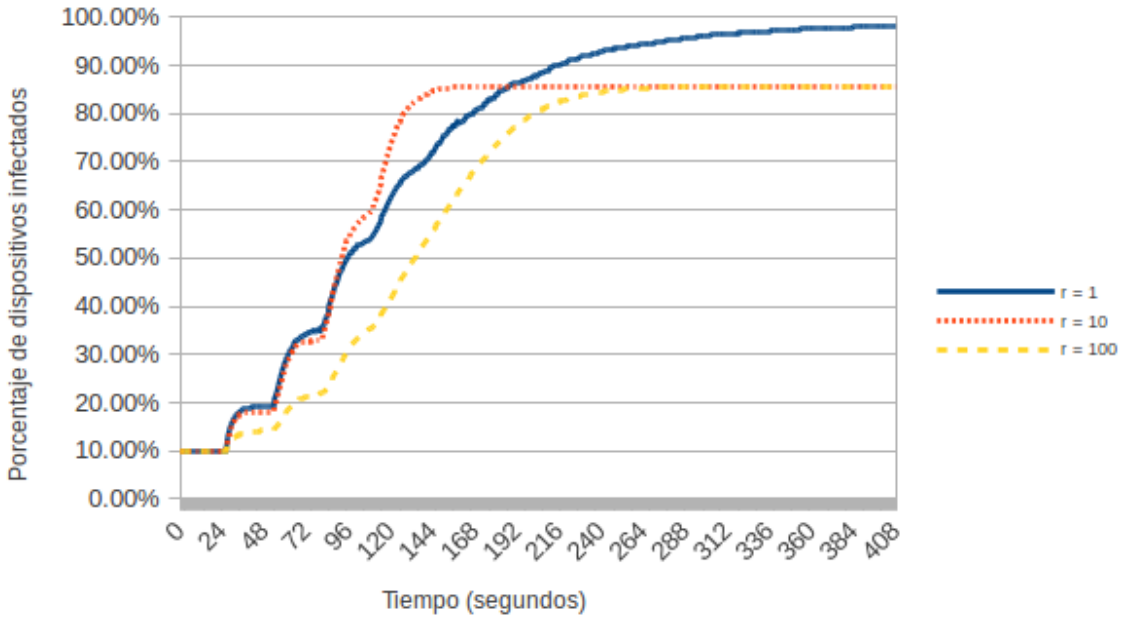


Fig. 4.17 - Comparación de la propagación del gusano para un radio r = 1, 10, 100 y una densidad σ = 50%

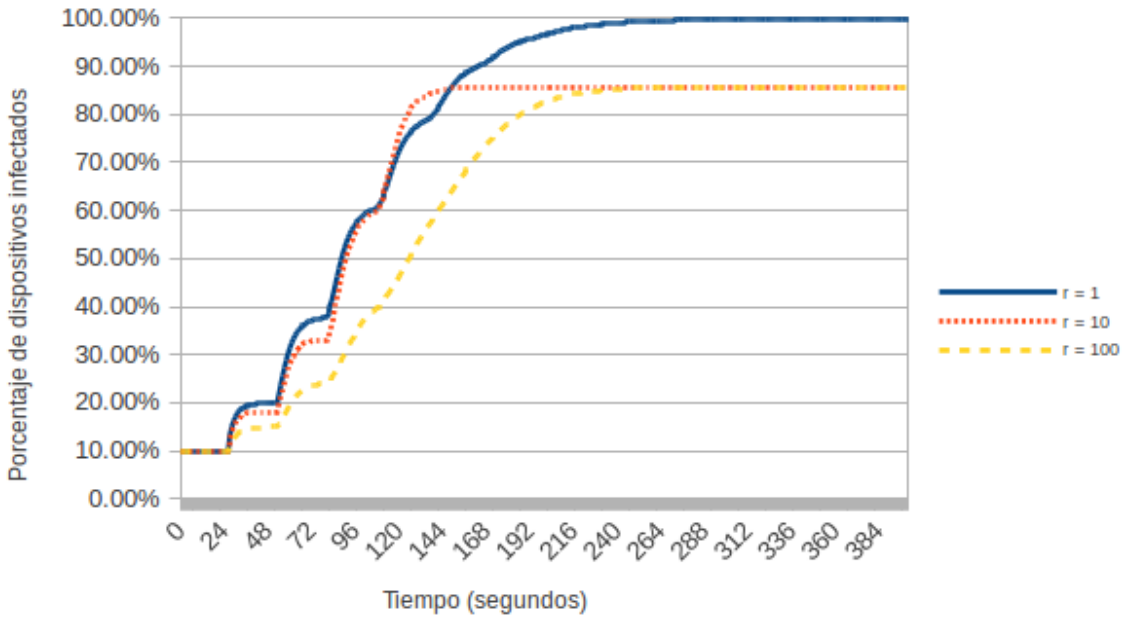


Fig. 4.18 - Comparación de la propagación del gusano para un radio r = 1, 10, 100 y una densidad σ = 60%

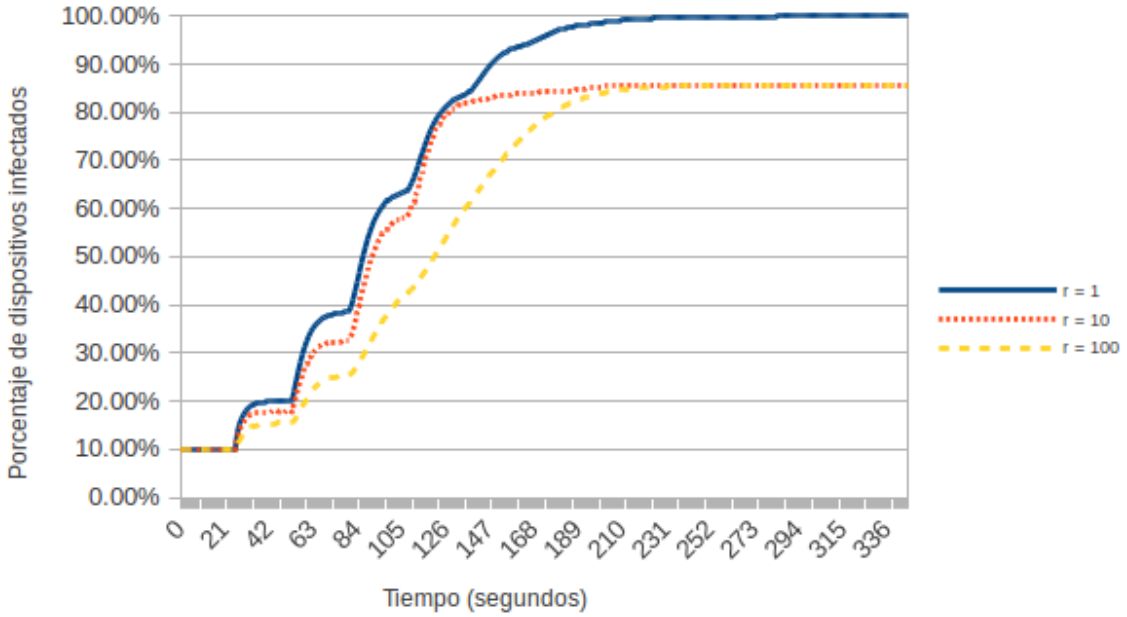


Fig. 4.19 - Comparación de la propagación del gusano para un radio r = 1, 10, 100 y una densidad σ = 70%

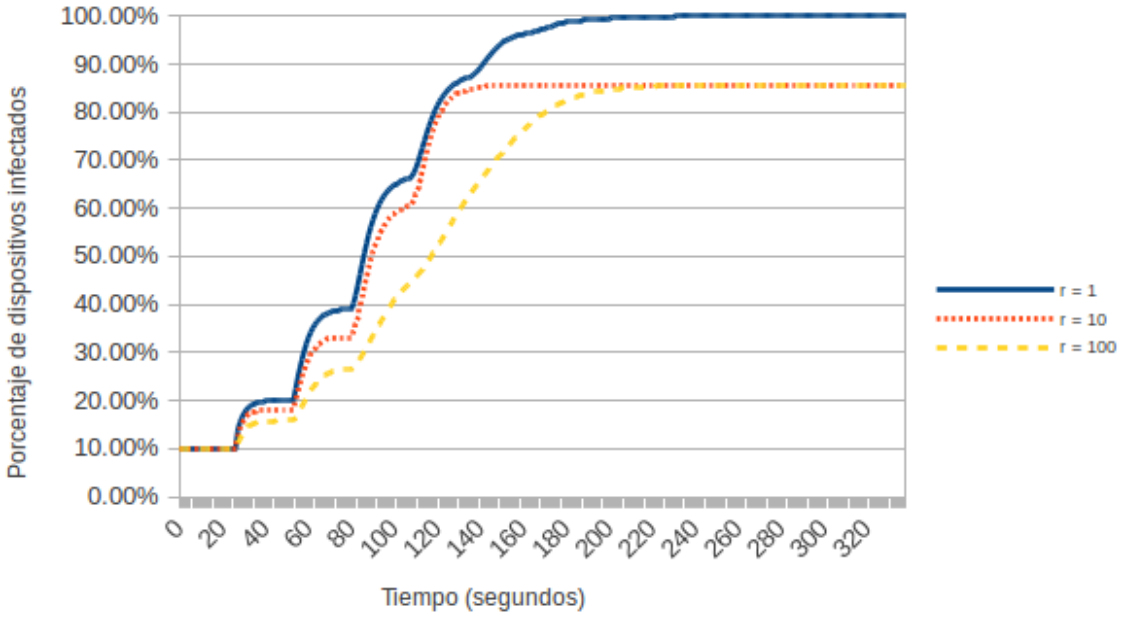


Fig. 4.20 - Comparación de la propagación del gusano para un radio r = 1, 10, 100 y una densidad σ = 80%

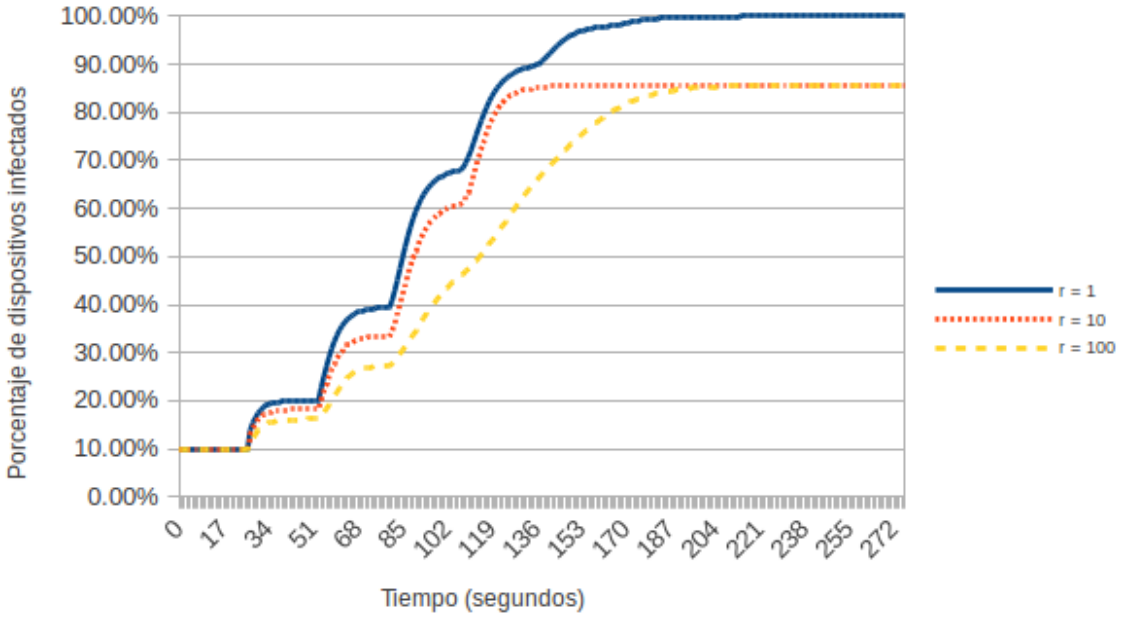


Fig. 4.21 - Comparación de la propagación del gusano para un radio r = 1, 10, 100 y una densidad σ = 90%

4.3 Resultados considerando movilidad

Uno de los factores críticos que influyen directamente en la dinámica de propagación de una enfermedad es el movimiento de los individuos. En el caso de los agentes biológicos, basta con que el virus sea transmitido del vector de infección al huésped susceptible mediante un contacto efectivo para hacerlo pasar a un estado de expuesto y terminado el tiempo de latencia o de

incubación finalmente llegara al estado de infectado. En muchas ocasiones el agente biológico y el individuo expuesto no necesitan permanecer juntos para que el proceso infeccioso se concluya como es el caso del dengue, en el que el mosquito puede morir antes de concluir el periodo de incubación de la enfermedad. En el caso de la propagación del malware tipo gusano a través de conexiones Bluetooth es necesario que, además del contacto efectivo, el dispositivo susceptible se mantenga en el rango de alcance de la antena Bluetooth del dispositivo infectado durante todo el tiempo de latencia requerido hasta que el malware sea transmitido por completo. Para modelar este evento, se introduce el estado de interrumpido (INT) que comprenderá a todos aquellos dispositivos expuestos que salieron del rango de transmisión del dispositivo infectado antes de completar la transmisión del gusano, posteriormente, los dispositivos en este estado regresarán nuevamente al estado susceptible.

Con la finalidad de aislar factores adicionales que pudieran perturbar la prueba, se elige una población homogénea de dispositivos, la probabilidad de diagnóstico P_2 y la probabilidad de remoción del gusano P_3 son asignadas a 0 (evento imposible), mientras que la probabilidad de que la antena Bluetooth este encendida ε y la probabilidad de aceptación de la conexión α son asignadas a 1 (evento seguro). De este modo el gusano tiene las condiciones adecuadas en cuanto a características de configuración de los dispositivos para una propagación efectiva, siendo la probabilidad de movimiento P_{MOV} la única variable que afecta esta dinámica. El resto de los parámetros empleados son mostrados en la Tabla 4.8.

Tipo de Población	Homogénea
Densidad (Número de dispositivos)	50%, 60%, 70%, 80%, 90%
Rango de la Antena Bluetooth	1
Número inicial de Infectados $I(0)$	10% de la población total
Probabilidad de Aceptación de conexión Bluetooth	1
Probabilidad de que la antena Bluetooth este encendida	1
Probabilidad de detección del Gusano P_2	0
Probabilidad de Remoción del Gusano P_3	0
Probabilidad de movimiento	0.10, 0.20, 0.30, 0.40, 0.50, 0.60, 0.70, 0.80, 0.90

Tabla 4.8 - Parámetros de prueba para la variación de la probabilidad de movimiento de los teléfonos inteligentes

Para validar el desempeño del modelo propuesto, se establece la comparación de dos escenarios: uno con una baja densidad de dispositivos y una alta probabilidad de movimiento y otro donde se tiene una alta densidad con una alta probabilidad de movimiento.

4.3.1 Caso 1: Baja densidad de dispositivos con alta probabilidad de movimiento

En la Fig. 4.22 , los resultados del primer caso son comparados con los resultados obtenidos en el experimento 4.2.1 (línea sólida), donde los dispositivos permanecen estáticos durante toda la simulación. Como se observa en la Fig. 4.22 correspondiente a una densidad de 50% y una probabilidad $P_{Mov} = 0.8$ (línea punteada), la movilidad de los teléfonos en el espacio simulado impacta significativamente la propagación del gusano, frenando la misma a pesar de que la población de teléfonos inteligentes no cuenta con ningún mecanismo de protección. Esto se debe a que el movimiento constante de los dispositivos en un área geográfica libre puede generar que se interrumpa permanentemente la transmisión del gusano, frenando la infección.

Los resultados del primer caso son comparados con los resultados obtenidos en el experimento 4.2.1 donde los dispositivos permanecen estáticos durante toda la simulación. Como se observa en la Fig. 4.22, el impacto de la movilidad en la dinámica de propagación del gusano es dramática, a pesar de que la población de teléfonos inteligentes no cuenta con ningún mecanismo de protección, el constante movimiento en un área geográfica libre hace que los dispositivos sean prácticamente inmunes al interrumpir permanentemente la transmisión del gusano, mientras que en el experimento 4.2.1 se infecta a más del 95% de la población en pocos pasos de tiempo.

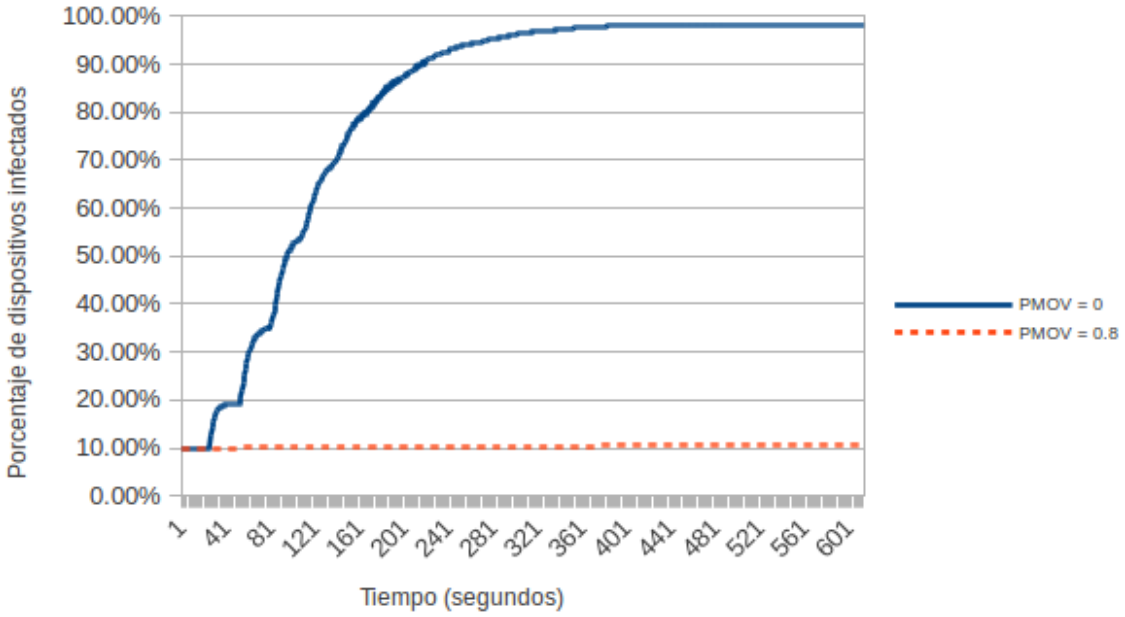


Fig. 4.22 - Comparación de la evolución de dispositivos infectados para una población homogénea con densidad σ = 50% y probabilidad de movimiento $P_{Mov} = 0{,}0.8$

Lo anterior refleja un comportamiento esperado dada la naturaleza de la comunicación a través de la antena Bluetooth. Para ilustrar el efecto de la movilidad se recurre al diagrama espacio-temporal del AC mostrado en la Fig. 4.23 que muestra la evolución del sistema en ciertos intervalos de tiempo de la simulación. Cada malla (imagen) representa el área geográfica simulada y su estado global en un instante del tiempo determinado y cada punto dentro de la malla representa a un teléfono inteligente cuyo color indica el estado del mismo de acuerdo al código de color descrito en la Tabla 4.9. De la Fig. 4.23 se observa como la distribución de los teléfonos inteligentes en el espacio celular

cambia drásticamente debido a la alta cantidad de células disponibles, lo cual afecta directamente a la dinámica de infección ya que la conexión entre un dispositivo susceptible y uno infectado, se verá interrumpida constantemente. Cabe recordar que los teléfonos que pasen al estado INT regresarán al estado de susceptible de forma incondicional en el tiempo $t + 1$.

Susceptible
Expuesto
Infectado
Interrumpido

Tabla 4.9 - Código de colores empleado en los diagramas espacio-temporales

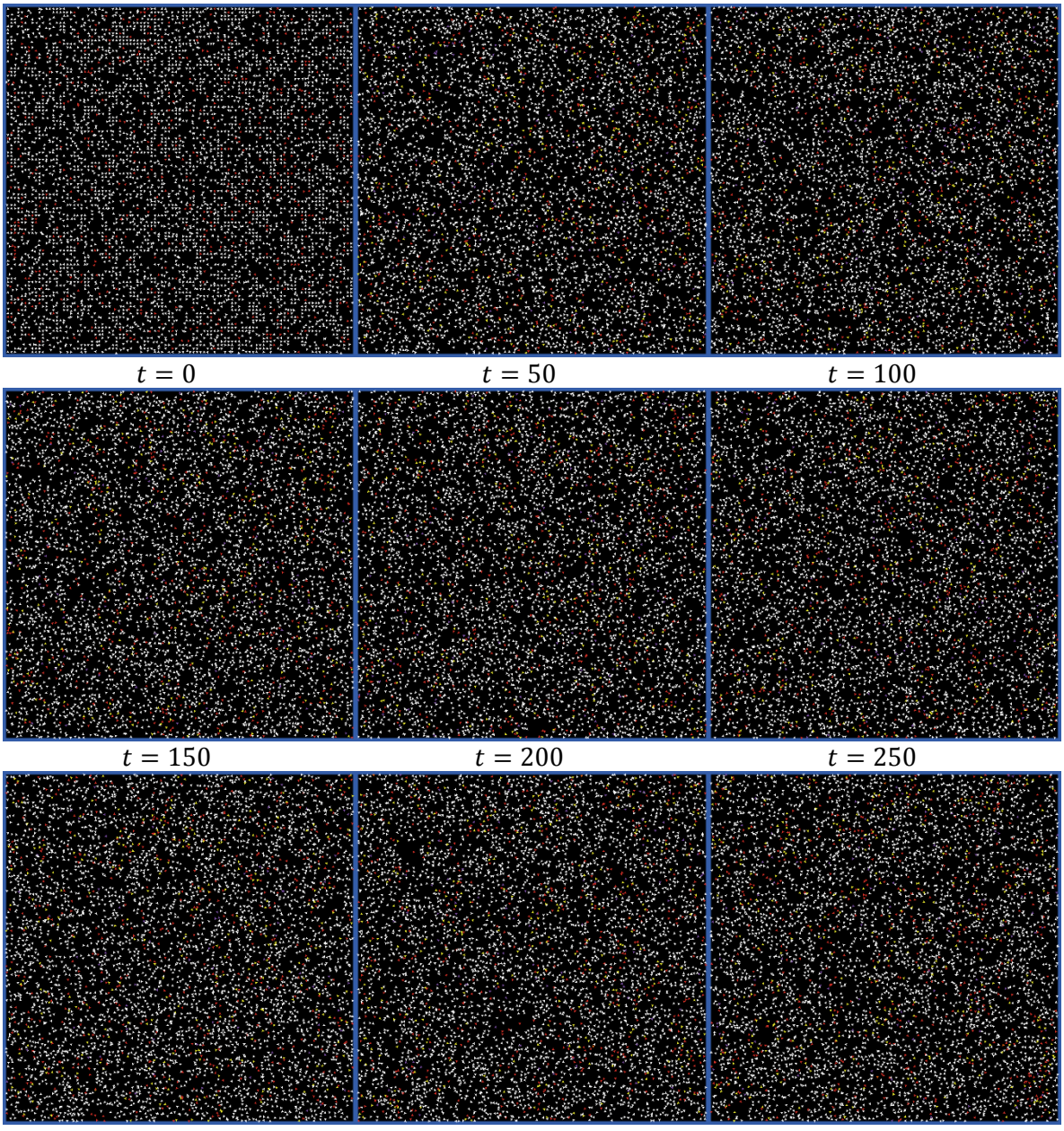


Fig. 4.23 - Diagrama espacio-temporal de propagación en una población homogénea con densidad ♂=50%, probabilidad de movimiento $P_{MOV} = 0.8$, probabilidad de diagnóstico y remoción del gusano $P_2 = P_3 = 0$ y probabilidad de aceptación y estado de la antena encendida $\propto = \varepsilon = 1$

4.3.2 Caso 2: Alta densidad de dispositivos con alta probabilidad de movimiento

De manera análoga al punto anterior, los resultados obtenidos en este caso son comparados con los resultados obtenidos en el experimento 4.2.1, en esta ocasión, la variación entre los dos experimentos no es tan grande como se da en las poblaciones con baja densidad. La Fig. 4.24 muestra que el porcentaje de dispositivos infectados para $P_{Mov} = 0$ y $P_{Mov} = 0.8$ y una densidad $\sigma = 90\%$. Como puede notarse, a diferencia de una densidad baja, el porcentaje de dispositivos infectados crece rápidamente independientemente del valor alto de P_{Mov}. Este comportamiento se debe a que a medida que la densidad se incrementa, se van reduciendo los espacios disponibles que un dispositivo tiene para moverse, por lo que los dispositivos terminan estando varios pasos de tiempo en el mismo lugar (semejante a $P_{Mov} = 0$); lo que favorece a la dinámica de propagación al no interrumpirse la conexión durante el proceso de infección.

Este caso de estudio puede representar situaciones reales con altas aglomeraciones por tiempos largos como conciertos, eventos deportivos, funciones de cine, etc. Al no haber ningún factor de resistencia en la población de teléfonos inteligentes y considerando que ésta es homogénea, la propagación del gusano se da en condiciones muy similares a como se dan cuando los dispositivos permanecen inmóviles.

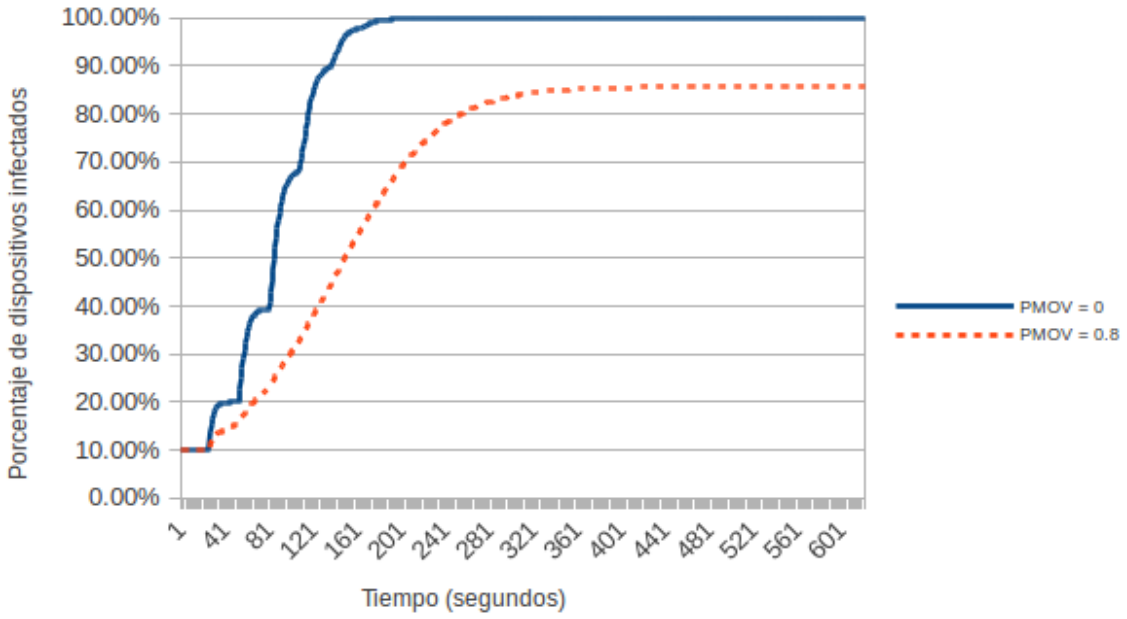


Fig. 4.24 - Comparación de la evolución de dispositivos infectados para una población homogénea con densidad σ = 90% y probabilidad de movimiento $P_{Mov} = 0{,}0.8$

La Fig. 4.25 muestra el diagrama espacio-temporal donde los dispositivos presentan movimiento como es de esperarse dada la probabilidad alta de que el evento suceda, asimismo se muestra como rápidamente el gusano se esparce en un tiempo promedio de 573 segundos. Se emplea el mismo código de colores mostrado en la Tabla 4.9.

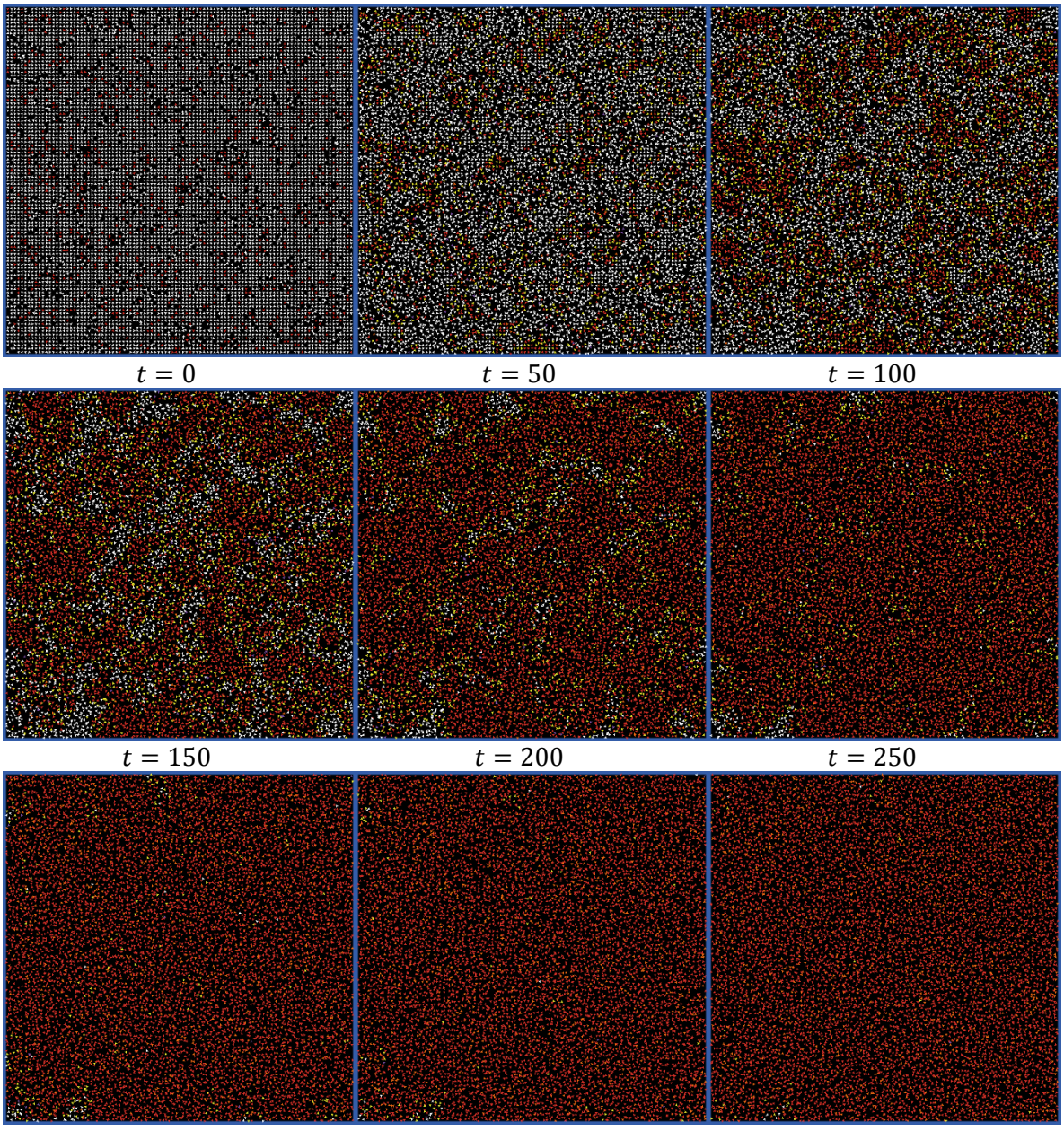


Fig. 4.25 - Diagrama espacio-temporal de propagación en una población homogénea con densidad ♂=90%, probabilidad de movimiento $P_{MOV} = 0.8$, probabilidad de diagnóstico y remoción del gusano $P_2 = P_3 = 0$ y probabilidad de aceptación y estado de la antena encendida $\propto = \varepsilon = 1$

La Fig. 4.26 muestra la baja incidencia de los dispositivos dentro del compartimento de interrumpido dadas las condiciones detalladas anteriormente.

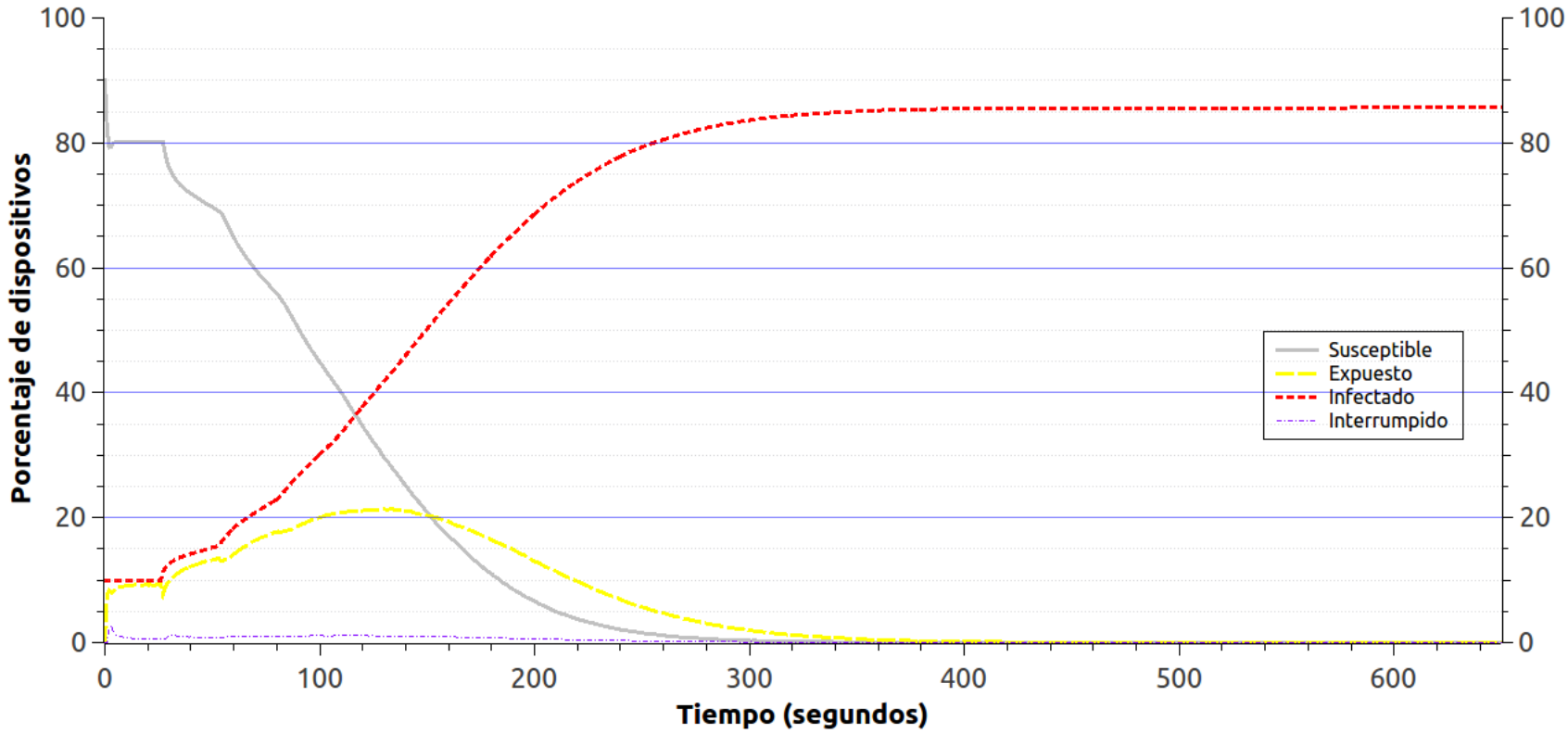


Fig. 4.26 - Evolución de los compartimentos una población homogénea con densidad σ = 90% y $P_{MOV} = 0.8$

Capítulo 5: Conclusiones y Trabajo Futuro

Los teléfonos móviles inteligentes son, a día de hoy, uno de los productos tecnológicos con mayor crecimiento en ventas de los últimos años. Este tipo de telefonía se caracteriza por ser un sistema de comunicación ampliamente difundido debido a su fácil acceso, conectividad y versatilidad. Se estima para el año 2016, el número de usuarios de estos dispositivos alcanzará una cifra aproximada de 2 billones. Sin embargo, los smartphones cuentan con sistemas operativos similares a una computadora, y tienen la ventaja del uso de redes geográficamente distribuidas a nivel global, facilitando el envío y recepción de correos electrónicos en cualquier momento, así como la realización de diversas transacciones online. Lo cual los hace vulnerables a riesgos derivados por virus o ataques informáticos y han llegado a ser uno de los objetivo principales para los desarrolladores de software malicioso (malware). El gran daño potencial que puede ser causado por el software malicioso ha motivado el desarrollo continuo de modelos para describir el proceso dinámico de la propagación de malware a través de teléfonos inteligentes con la finalidad de entender el mecanismo de propagación del malware, predecir su escala propagación, evaluar sus impactos, caracterizar su dinámica de infección y diseñar medidas de control para restringir su propagación.

Uno de los medios de transmisión de malware en los teléfonos inteligentes es Bluetooth. En este trabajo de tesis, se introdujo un nuevo modelo discreto basado en Autómatas Celulares (AC) y las teorías epidemiológicas de los modelos matemáticos compartimentales para la simulación de la propagación espacio-temporal de malware de tipo gusano a través de conexiones Bluetooth en teléfonos inteligentes. El nuevo modelo toma en cuenta aspectos relevantes en el estudio del tema y que no han sido considerados en otros modelos existentes en la literatura, tales como: los efectos de la resistencia al gusano por características inherentes a un tipo de población (por ejemplo, tipo de sistema operativo), estudio de un área geográfica de cualquier tamaño, movimiento de los dispositivos dentro del espacio geográfico establecido para el análisis de las conexiones interrumpidas y su repercusión en la dinámica de propagación del malware cuyo vector de infección son antenas Bluetooth. Resultados de simulación sobre áreas geográficas de pequeñas a medianas indican que el modelo propuesto en este trabajo es computacionalmente simple y adecuado para su uso en predicción y evaluación del desempeño de propagación de malware.

Los casos de estudio considerados en este trabajo describen situaciones reales donde ciertas características de un teléfono influyen de manera particular en la mecánica de propagación del

gusano. Los estudios se dividieron en dos grandes grupos: pruebas considerando que los dispositivos se mantienen estáticos durante toda la simulación y en pruebas donde se define un rango de probabilidad de movimiento. La finalidad de estos grupos de estudio fue estudiar cómo es que la probabilidad de movimiento influye en la propagación del gusano y a diferencia de los virus biológicos, una probabilidad alta de movimiento en un espacio con múltiples células libres, frena el esparcimiento del gusano dado el requerimiento de proximidad para la comunicación entre los teléfonos. Incluso, sin un factor de diagnóstico ni remoción, el estado de los teléfonos se mantiene oscilando entre expuesto y susceptible (estado alcanzado a través de la transición de expuesto a interrumpido).

Los resultados de simulación sin considerar movilidad indican que cuando la densidad de los dispositivos en un espacio geográfico es menor a la mitad y las antenas Bluetooth de los dispositivos tienen un radio de alcance corto (*r=1*), el gusano no es capaz de propagarse a todos los dispositivos dado que los espacios entre ellos forman cercos que frenan la propagación del gusano. Conforme el radio de transmisión *r* aumenta, la propagación del gusano se acelera hasta que el sistema se satura, se determinó que a mayor rango de transmisión *r*, la probabilidad de que las vecindades de los teléfonos infectados se traslape también aumenta, lo cual hace que la propagación del gusano no pueda continuar a la misma velocidad ni con la misma eficiencia que en un radio corto. Por otra parte se encontró que, como era de esperarse, el impacto del estado de la antena Bluetooth (encendido o apagado) es determinante en la propagación del gusano, si la antena se encuentra apagada, el dispositivo es inmune al gusano. Por tal motivo, el uso de teléfonos susceptibles con la antena apagada como valores asignados en la frontera del espacio celular fue adecuado para delimitar este espacio. Adicionalmente, dada la función lógica que determina el contacto efectivo entre un teléfono infectado y uno susceptible, se requiere que el teléfono susceptible además de contar con la antena encendida, acepte la solicitud de conexión. Esta condición lógica hace que los resultados de variar únicamente la probabilidad de aceptación de la conexión entrante sean los mismos a cuando sólo se varía la probabilidad de que la antena Bluetooth se encuentre encendida. Adicionalmente, resultados considerando una población de teléfonos heterogénea con diferente sistema operativo indican que el desempeño del modelo y su propagación es consistente y adecuado.

Uno de los temas más relevantes en el desarrollo de este trabajo fue el estudio de los mecanismos de control para detener la propagación del malware. Se observó que entre los incrementos de 0.1 iniciando para una probabilidad inicial de diagnóstico y remoción de 0.1, la velocidad de propagación del gusano se ve fuertemente afectada. Se determinó que estas probabilidades con valores bajos, el sistema toma mucho más tiempo (casi 21,600 segundos) en estabilizarse pero al hacerlo, todos los teléfonos infectados son diagnosticados y recuperados. El sistema llega al estado de equilibro dado que no se consideran factores de renovación y por ende, el gusano es eliminado de la red de teléfonos inteligentes al paso de este tiempo.

Por otro lado, resultados de simulación considerando movilidad espacial de los teléfonos indican que el modelo es adecuado para estudiar y analizar comportamientos de la dinámica de infección en el tiempo derivados comportamientos individuales de los teléfonos.

Finalmente, el modelo propuesto mantiene la simplicidad en sus reglas de transición entre los estados definidos, la naturaleza del AC permite que sea computacionalmente paralelizable lo que lo hace adecuado para simular áreas geográficas grandes.

5.1 Trabajo Futuro

El modelo presentado en este trabajo se enfoca solamente a transmisión de virus en teléfonos inteligentes a través de Bluetooth. Sin embargo, los malware también puede transmitirse a través de SMS, MMS y otros, los cuales quedaron fueran del alcance de este trabajo, pero el modelo puede adaptarse en forma simple para ello.

Por otra parte, debido a que el modelo propuesto se basa en AC, es posible a través del mismo llevar un registro histórico de la cadena de infección de cada uno de los dispositivos, es decir, llevar un registro de que teléfono infecto a otro. Esta característica podría ser útil en el estudio del origen de la infección para el estudio forense, desde el punto de vista de seguridad en cómputo.

Aunque en este trabajo de tesis sólo se presentan resultados basados en simulación computacional del modelo propuesto, es de gran importancia su comparación con otro tipo de datos, como los resultantes de un simulador o datos reales, estos últimos no se lograron conseguir.

Por otra parte, La implementación computacional actual del modelo para su estudio y evaluación fue desarrollada en NetLogo, dadas las características ofrecidas por este lenguaje tales como, manejo de agentes y paradigma de programación funcional. Sin embargo, para el estudio de áreas geográficas grandes y su aplicación real el uso de un lenguaje de programación de alto nivel como Java nativo o C++ permitiría una mejor aplicación del mismo. Queda como trabajo futuro la migración de la implementación del modelo a otro lenguaje de programación orientado a objetos para incrementar el desempeño.

Referencias

[1] J. Kurose and K. Ross, Computer Networking A Top-Down Approach 6th Edition, Pearson, 2012.

[2] S. Curtis, "Quarter of the world will be using smartphones in 2016," 11 12 2014. [Online]. Available: http://www.telegraph.co.uk/technology/mobile-phones/11287659/Quarter-of-the-world-will-be-using-smartphones-in-2016.html. [Accessed 27 Abril 2015].

[3] H. Xiang, *Bluetooth-Base Worm Modeling and Simulation,* 1998.

[4] R. Nuwer, «Why is Bluetooth Called Bluetooth?,» Smithsonian, 27 Agosto 2012. [En línea]. Available: http://www.smithsonianmag.com/smart-news/why-is-bluetooth-called-bluetooth-hint-vikings-16270647/?no-ist. [Último acceso: 2 Septiembre 2015].

[5] C. Shin-Ming, C. A. Weng, C. Pin-Yu and C. Kwang-Cheng, "On Modeling Malware Propagation in Generalized Social Networks," *Communications Letters, IEEE ,* vol. 15, no. 1, pp. 25 - 27, 2011.

[6] J. Jackson y S. Creese, «Virus Propagation in Heterogeneous Bluetooth Networks with Human Behaviors,» *Dependable and Secure Computing, IEEE Transactions,* vol. 9, nº 6, pp. 930 - 943, 2012.

[7] J. Mickens y B. Noble, «Modeling Epidemic Spreading in Mobile Environments,» de *Proceedings of the ACM Workshop on Wireless Security*, 2007.

[8] A. Fúster, Á. M. Del Rey y G. Rodríguez, «Simulación de la propagación del malware: modelos continuos vs. modelos discretos,» de *Actas de la XIII Reunión Española sobre Criptología y Seguridad de la Información*, Alicante, 2014.

[9] Á. Martín del Rey y G. Rodríguez Sánchez, «A CA Model for Mobile Malware Spreading Based on Bluetooth Connections,» *International Joint Conference SOCO'13-CISIS'13-ICEUTE'13,* vol. 239, nº Springer International Publishing, pp. pp 619-629, 2014.

[10] M. Frodigh, P. Johansson y P. Larsson, «Wireless ad hoc networking - The art of networking without a network,» 2000. [En línea]. Available: http://www.ericsson.com/ericsson/corpinfo/publications/review/2000_04/files/2000046.pdf. [Último acceso: 1 Septiembre 2015].

[11] S. Glisic y B. Lorenzo, Advanced Wireless Networks: 4G technologies, Wiley, 2009.

[12] Bluetooth SIG, «Fast Facts | Bluetooth Technology,» Bluetooth SIG, 2015. [En línea]. Available: http://www.bluetooth.com/Pages/Fast-Facts.aspx. [Último acceso: 2 Septiembre 2015].

[13] IEEE Computer Society, *802.15.1 Part 15.1: Wireless medium access control (MAC) and physical layer (PHY) specifications for wireless personal area networks (WPANs),* New York, 2005.

[14] Ericsson Technology Licensing, «Scatternet - Part 1: Baseband vs. Host Stack Implementation,» Ericsson Technology Licensing, 2004.

[15] F. Cohen, A short course on computer viruses, New York: Wiley Professonal Computing, 1994.

[16] P. Szor, The Art of Computer Virus Research and Defense, Addison Wesley Professional, 2005.

[17] V. Bontchev, «Current Status of the CARO,» 13 Octubre 2005. [En línea]. Available: https://www.virusbtn.com/pdf/conference_slides/2005/Vesselin%20Bontchev.pdf. [Último acceso: 6 Septiembre 2015].

[18] BitDefender, «http://www.bitdefender.com/,» 10 Abril 2010. [En línea]. Available: http://download.bitdefender.com/resources/files/Main/file/Malware_History.pdf. [Último acceso: 10 Septiembre 2015].

[19] Computer Economics, «http://www.computereconomics.com,» Computer Economics, Junio 2007. [En línea]. Available: http://www.computereconomics.com/article.cfm?id=1225. [Último acceso: 10 Septiembre 2015].

[20] Center for Strategic and International Studies, «Net Losses: Estimating the Global Cost of Cybercrime,» McAfee, 2014.

[21] G. Yan y S. Eidenbenz, «Modeling Propagation Dynamics of Bluetooth Worms,» de *Distributed Computing Systems, 2007. ICDCS '07. 27th International Conference*, Toronto, ON, 2007.

[22] H. W. Hethcote, «Three Basic Epidemiological Models,» de *Applied Mathematical Ecology*, S. A. Levin, T. G. Hallam y L. J. Gross, Edits., Springer Berlin Heidelberg, 1989, pp. pp 119-144.

[23] W. Kermack y A. McKendrick, «A Contribution to the Mathematical Theory of Epidemics,» de *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 1927.

[24] W. Kermack y A. McKendrick, «Contribution to the Mathematical Theory of Epidemics II: The problem of Endemicity,» de *Proccedings of the Royal Society of London*, 1932.

[25] W. Kermack y A. McKendrick, «Contribution to the Mathematical Theory of Epidemics III: Further Studies of the Problem of Endemicity,» de *Proceedings of the Royal Society*, 1933.

[26] S. Peng, S. Yu y A. Yang, «Smartphone Malware and its Propagation Modeling: a Survey,» *IEEE Communications Surveys & Tutorials,* vol. 16, nº 2, pp. 925 - 941, 2014.

[27] J. Von Neumann y A. Burks, Theory of Self-Reproducing Automata, Illinois: University of Illinois Press, 1966.

[28] G. Juárez Martinez, A. Adamatzky y H. McIntosh, «Localization dynamic in binary two-dimensional cellular automaton: Diffusion Rule,» *Journal of Cellular Automata,* vol. 5, nº 4/5, pp. 289-313, 2010.

[29] C. J. Rhodes y M. Nekovee, «The opportunistic transmission of wireless worms between mobile devices,» *Physica A: Statistical Mechanics and its Applications,* vol. 387, nº 27, pp. 6837-6844, 2008.

[30] J. C. Martin, L. L. I. Burge, J. I. Gill, A. N. Washington y M. Alfred, «Modelling the spread of mobile malware,» *International J. Computer Aided Engineering and Technology,* vol. 2, nº 1, pp. 3-14, 2010.

[31] K. Ramachandran y B. Sikdar, «Modeling malware propagation in networks of smart cell phones with spatial dynamics,» de *Proc. 26th IEEE International Conference on Computer Communications (INFOCOM 2007)*, Anchorage, 2007.

[32] X. Wei, L. Zhao-hui, C. Zeng-qiang y Y. Zhu-zhi, «Commwarrior worm propagation model for smart phone networks,» *The Journal of China Universities of Posts and Telecommunications,* vol. 15, nº 2, pp. 60-66, 2008.

[33] S. Peng, G. Wang y S. Yu, «Modeling the Dynamics of Worm Propagation using Two-dimensional Cellular Automata in Smartphones,» *Journal of Computer and System Sciences,* 2012.

[34] S. Peng y G. Wang, «Worm Propagation Modeling Using 2D Cellular Automata in Bluetooth Networks,» de *International Joint Conference of IEEE TrustCom-11/IEEE ICESS-11/FCST-11*, 2011.

[35] Z. Bakhshi, M. Lighvan y R. Mostafavi, «MP-CA: Malware Propagation Modeling Methodology Based on Cellular Automata,» *International Journal of Computer Networks and Communications Security,* vol. 3, nº 3, p. 63–73, 2015.

[36] A. Martín del Rey, A. Hernández Encinas, J. Martín Vaquero, A. Queiruga Dios y G. Rodríguez Sánchez, «A Cellular Automata Model for Mobile Worm Propagation,» de *Bioinspired Computation in Artificial Systems*, Switzerland, Springer International Publishing, 2015, pp. 107-116.

[37] G. Zyba, «Mobile Malware Propagation and Defense,» 2013. [En línea]. Available: http://escholarship.org/uc/item/65k426wt. [Último acceso: 11 Abril 2016].

[38] Statista, «Mobile OS market share 2016 | Statistic,» Statista, 2016. [En línea]. Available: http://www.statista.com/statistics/266136/global-market-share-held-by-smartphone-operating-systems/. [Último acceso: 25 Julio 2016].

[39] A. S. Tanenbaum, Computer networks, Seattle, WA: Pretince Hall, 2011.

[40] E. Kaspersky, «10 years since the first smartphone malware – to the day,» 15 Junio 2014. [En línea]. Available: http://eugene.kaspersky.com/2014/06/15/10-years-since-the-first-smartphone-malware-to-the-minute/. [Último acceso: 07 05 2015].

[41] Y. Hu, J. Yu y F. Zong, «Cellular Automata Model to Simulate the Spreading of Mobile Phone Messages Virus,» *Journal of Information & Computational Science,* vol. 10, nº 11, 2013.

[42] «Bluetooth | Android Developers,» [En línea]. Available: http://developer.android.com/guide/topics/connectivity/bluetooth.html. [Último acceso: 23 Mayo 2015].

[43] J. Vacca, «Wireless Data Demystified,» McGraw-Hill, 2003, p. 490.

[44] F. Brauer, «Compartmental Models in Epidemiology,» de *Mathematical Epidemiology*, Springer Berlin Heidelberg, 2008, pp. 19-79.

[45] Centers for Disease Control and Prevention, «SARS | Basics Factsheet | CDC,» Centers for Disease Control and Prevention, 3 Mayo 2005. [En línea]. Available: http://www.cdc.gov/sars/about/fs-sars.html. [Último acceso: 23 Septiembre 2015].

[46] Centers for Disease Control and Prevention, «2014 Ebola Outbreak in West Africa | Ebola Hemorrhagic Fever | CDC,» Centers for Disease Control and Prevention, 23 Septiembre 2015. [En línea]. Available: http://www.cdc.gov/vhf/ebola/outbreaks/2014-west-africa/index.html. [Último acceso: 23 Seotiembre 2015].

[47] W. Ning-Ning y C. Guo-Long, «A Virus Spread Model Based on Cellular Automata in Weighted Scale-Free Networks,» de *Proceedings of the 2012 International Conference on Communication, Electronics and Automation Engineering*, Springer Berlin Heidelberg, 2013, pp. 1169-1175.

[48] E. W. Weisstein, «Moore Neighborhood,» Wolfram MathWorld, 21 Enero 2003. [En línea]. Available: http://mathworld.wolfram.com/MooreNeighborhood.html. [Último acceso: 28 10 2015].

[49] Y. Song y G. Ping Jiang, «Modeling marlware propagation in wireless Sensor Networks using Cellular Automata,» de *IEEE Int. Conference Neural Networks & Signal Processing*, 2008.

[50] Y. Song y G.-P. Jang, «Modeling Malware Propagation in Wireless Sensor Networks using Cellular Automata,» de *Conference Neural Networks & Signal Processing*, Zhenjiang, 2008.

[51] N. Valler, A. Prakash, H. Tong, M. Faloutsos y C. Faloutsos, «Epidemic Spread in Mobile Ad Hoc Networks,» de *Networking 2011*, Springer Berlin Heidelberg, 2011, pp. 266-280.

[52] C. Gao y J. Liu, «Modeling and Predicting the Dynamics of Mobile Virus Spread Affected by Human Behavior,» de *Proc. 12th IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM 2011)*, Lucca, Italy, 2011.

[53] P. Wang, M. C. Gonzalez y C. A. Hidalgo, «Understanding the spreading patterns of mobile phone viruses,» *Science,* vol. 324, nº 5930, pp. 1071-1076, 2009.