
UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

POSGRADO EN CIENCIA E INGENIERÍA EN COMPUTACIÓN
INSTITUTO DE INVESTIGACIONES EN MATEMÁTICAS APLICADAS Y EN SISTEMAS

# MODELO DE PROPAGACIÓN DE MALWARE HÍBRIDO EN REDES COMPUTACIONALES BASADO EN AUTÓMATAS CELULARES CONSIDERANDO EL COMPORTAMIENTO HUMANO

Tesis

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

PRESENTA:
Mtro. Gabriel González García

Tutor:
Dra. María Elena Lárraga Ramírez
Instituto de Ingeniería

Ciudad Universitaria, Cd. Mx. Julio 2022

# Resumen

El uso de los teléfonos inteligentes se ha convertido en una parte inherente de la vida diaria del ser humano. Permite a los usuarios guardar información personal, correos electrónicos, fotos, cuentas de redes sociales y datos financieros en un solo lugar. En consecuencia, los teléfonos inteligentes se han convertido en un objetivo atractivo para que los desarrolladores de malware propaguen contenidos maliciosos, con el objetivo de extraer información sin que el usuario lo sepa. Por lo tanto, comprender las características de propagación de los programas maliciosos podría proporcionar un medio para evaluar su comportamiento con el fin de planificar soluciones de seguridad. Las antenas Bluetooth son un canal de propagación de malware a través de los smartphones, donde la probabilidad de infección depende principalmente de la proximidad física del atacante de forma similar a la de los virus biológicos. Este trabajo presenta un modelo basado en autómatas celulares y modelos epidemiológicos compartimentales para estudiar la propagación espacio-temporal de gusanos Bluetooth en smartphones. El modelo propuesto incorpora las características individuales de cada dispositivo, como la configuración de seguridad, el tiempo de latencia, el sistema operativo, las diferentes clases de antenas Bluetooth (alcance y tasa de transferencia) y los diferentes patrones de movilidad de los usuarios. Se analizan varios escenarios de simulación para estudiar la dinámica de propagación de gusanos basados en Bluetooth, teniendo en cuenta el lugar donde se inicia el brote y los diferentes tipos de antenas integradas en los dispositivos inteligentes. Los resultados de la simulación indican que el modelo propuesto es apropiado

para estudiar cómo la demografía de los usuarios afecta a la dinámica de propagación del gusano en el tiempo y el espacio. Además, el modelo permite analizar el impacto de la conciencia de los usuarios sobre los riesgos inherentes al uso de dispositivos inteligentes en redes Bluetooth, en función de la aceptación de la comunicación entrante y de los efectos de recuperación e inmunidad a las amenazas. Por último, el modelo propuesto conserva la simplicidad y la eficiencia computacional, con la posibilidad de extenderse más allá de Bluetooth para incluir otros medios de transmisión.

# Abstract

The use of smartphones has become an inherent part of daily human life. It allows users to keep personal information, emails, pictures, social media accounts, and financial data in one place. Consequently, smartphones are an attractive target for malware developers to spread malicious content, aiming at extracting information without the user's knowledge. Therefore, understanding malware propagation characteristics could provide a means to evaluate how they behave in order to plan security solutions accordingly. Bluetooth antennas are a channel for spreading malware through smartphones, where the probability of infection, similar to biological viruses, depends mainly on the attacker's physical proximity. This work presents a model based on cellular automata and epidemiological compartmental models for studying the spatial and temporal propagation of Bluetooth worms in smartphones. The proposed model incorporates the individual characteristics of each device, such as security settings, latency time, operating system, different classes of Bluetooth antennas (range and transfer rate), and different user mobility patterns. Several simulation scenarios are analyzed in order to study the spreading dynamics of Bluetooth-based worms, considering the location where the outbreak begins, and the different types of antennas integrated into the smart devices. Simulation results indicated that the proposed model is appropriate for studying how the users' demographics affect the worm's propagation dynamics in time and space. Moreover, the model permits an analysis of the impact of users' awareness about the risks inherent in using smart devices in Bluetooth networks, based on the acceptance of incoming

communication and the effects of recovery and immunity to threats. Finally, the proposed model preserves simplicity and computational efficiency, with the possibility of extending beyond Bluetooth in order to include other transmission media.

# Agradecimientos

A mis sinodales, los doctores Francisco García y Oscar Arana por haber compartido conmigo su valiosa experiencia y entusiasmo sobre el tema y haber enriquecido este trabajo.

A mi comité tutor, la Dra. María Elena Lárraga Ramírez (tutora), Dr. Luis Álvarez-Icaza y Dr. Javier Gómez por su esfuerzo, tiempo y dedicación puestos en el desarrollo de este trabajo, así como los consejos que me dieron para mejorarlo 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 un doctorado de excelencia; al Consejo Nacional de Ciencia y Tecnología (CONACyT) la beca que se me otorgó para la realización de mis estudios de doctorado y finalmente a los proyectos PAPIIT_DGAPA IN112716 y IN101922 por el apoyo otorgado para la realización de este trabajo de tesis y su difusión.

# Índice general

# 1 Introducción

Hoy en día, Internet es el mayor sistema de ingeniería jamás creado, con cientos de millones de equipos de cómputo conectados mediante diversos enlaces de comunicación, con miles de millones de usuarios que se conectan empleando computadoras portátiles (laptops), tabletas, teléfonos inteligentes y con una serie de diversos dispositivos conectados a Internet tales como sensores, cámaras web, consolas de videojuegos, 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]. Hasta hace poco 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. Este hecho, aunado al alto consumo 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 con Statista, el número de usuarios de estos dispositivos alcanzó los 6.56 miles de millones en 2022 [2]. De tal manera que los teléfonos inteligentes tienen un rol importante en la vida laboral y personal, ya que no solo se usan para comunicarse mediante lla-

madas 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 y no oficiales, cuyas funcionalidades se encuentran en un amplio rango. Sin embargo, la mayoría de las aplicaciones requieren acceso a internet y en consecuencia, los dispositivos están expuestos a los efectos de amenazas, como el software orientado a infiltrarse o dañar una computadora o sistema de información sin el consentimiento de su propietario (nombrado *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. De éstos, los caballos de Troya se catalogan como la amenaza más frecuente ocupando el 85 % de las amenazas detectadas [3]; sin embargo, su proceso infeccioso no iniciará hasta que el usuario ejecute manualmente el archivo malicioso. Por tal razón, este trabajo se enfoca en el *malware* tipo gusano, el cual no necesita la intervención del usuario para infectar un equipo. Cabir fue el primer gusano para teléfonos inteligentes reportado en 2004 [4]. Las consecuencias del *malware* o virus en dispositivos inteligentes pueden ir desde la duración reducida de la batería, anuncios no deseados, la degradación del funcionamiento del dispositivo, el 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 múltiples modelos para describir el proceso dinámico de su propagación. Los objetivos de estos modelos de propagación se pueden clasificar en las siguientes categorías: (1) obtener una comprensión profunda de los mecanismos de propagación; (2) predecir la escala del contagio del *malware* antes de que realmente ocurra; (3) caracterizar la dinámica de infección del *malware*; y (4) diseñar y evaluar el funcionamiento de las contramedidas para frenar su propagación.

## 1.1. Definición del problema

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 éste mediante el uso de teorías de epidemia clásicas; ello debido a la fuerte semejanza en el desempeño 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 [5–7]. Aunque estos modelos continuos tienen una base matemática sólida que permite un estudio cualitativo muy detallado, 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.

Por tal razón, recientemente, 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) [9–11]; 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 de seguridad y operacionales semejantes, y que la transmisión del gusano se realiza en un solo paso de tiempo, lo que se aleja del desempeño real. Recientemente, Martín del Rey et al. [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.

## 1.2. Hipótesis

Es posible simular de forma fiel y simple la propagación de malware tipo gusano cuyo vector de infección depende de la proximidad física con otros dispositivos, mediante el uso del paradigma de AC, agentes y ciencia de redes.

## 1.3. Metas

### 1.3.1. Meta general

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, etc.

### 1.3.2. Metas particulares

- Proponer un modelo que permita extender las el trabajo [12] para considerar capacidades que permitan tener una abstracción más cercana al fenómeno real.

- Mostrar y validar la efectividad del modelo propuesto al realizar simulaciones computacionales del mismo.

- Realizar 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.

- Determinar cuáles son las condiciones que favorecen o contienen la propagación de malware tipo gusano en una red de dispositivos.

## 1.4. Descripción del contenido

En el capítulo 2, se introduce al lector en los términos relacionados con el trabajo de tesis para un mejor entendimiento y comprensión del mismo. En el capítulo 3, se presenta una breve revisión de trabajos relacionados con este trabajo de tesis. En el capítulo 4, se presenta un modelo nuevo para describir la propagación de *malware* tipo gusano en teléfonos inteligentes a través de Bluetooth. En el capítulo 5, se presenta una validación y verificación del desempeño del modelo mediante simulación computacional. Finalmente, en el capítulo 6 se presentan las conclusiones de este trabajo de tesis y algunas propuestas para trabajo futuro.

# 2

# Malware y Redes Bluetooth

En este capítulo, se define 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; junto con la definición de los Autómatas Celulares, que ayudaran a que el lector tenga una mejor comprensión de la descripción de los antecedentes de este trabajo que se presentan en el capítulo 2.

## 2.1. Introducción

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. Este hecho, aunado al alto consumo de 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 (smartphones en inglés) se ha incrementado a un ritmo vertiginoso; de acuerdo con Statista, el número de usuarios de estos dispositivos alcanzó los 6.56 miles de millones en 2022 [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 fotográfica, antena Bluetooth, Wi-Fi, navegadores web, correo electrónico, acceso a redes sociales, aplicaciones, reproductor de videos y música. Lo más importante, se almacenan una gran cantidad de datos personales en ellos. Dichas capacidades, así como el gran crecimiento en su disponibilidad y uso, han generado que los teléfonos inteligentes sean también un objetivo atractivo para los desarrolladores 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.

## 2.2. Medios de Transmisión Alternativos

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

### 2.2.1. Redes Ad-hoc

Una red Ad-hoc es una red que no posee un control central y en algunas ocasiones, no tiene salida a Internet. Esta red es formada dinámicamente 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 figura. 2.1 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.

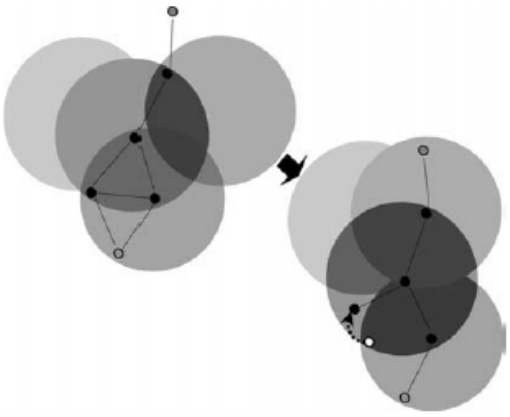


Figura 2.1: Topología dinámica de una red Ad-hoc

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

#### 2.2.1.1. 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* [4]. 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 solo 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, 13].

Por su extensión, una red Bluetooh pertenece a la clasificación de redes WPAN (Wide Personal Area Network) 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 [14].

#### 2.2.1.2. 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 figura. 2.2. El nodo maestro es el que gobierna la Piconet, su reloj coordina el tiempo dentro de la Piconet y solo puede transmitir datos a un nodo esclavo en cada ranura de tiempo impar. Así, los nodos esclavos pueden transmitir datos solo 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.

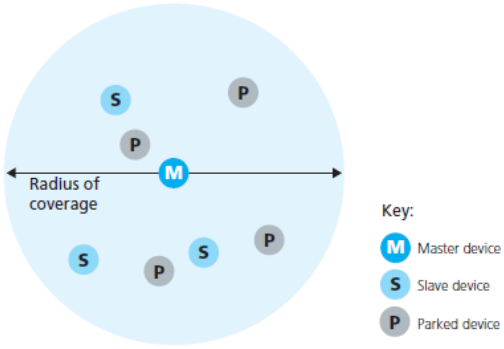



Figura 2.2: Ejemplo de una Piconet Bluetooth. Imagen tomada de [1]

.

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 solo dispositivo Bluetooth puede participar como esclavo en varias piconets pero solo puede actuar como maestro en una piconet [15] como se muestra en la fig 2.3.

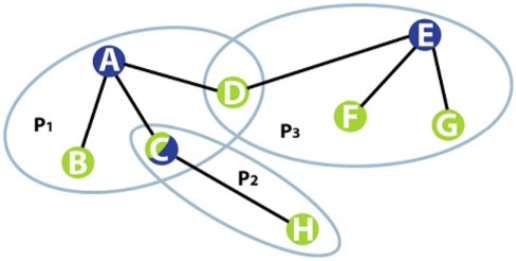



Figura 2.3: Ejemplo de Scatternet Bluetooth. Imagen tomada de [15]

La figura 2.3 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 $P_2$.

#### 2.2.1.3. 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, 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 figura 2.4 muestra un ejemplo:

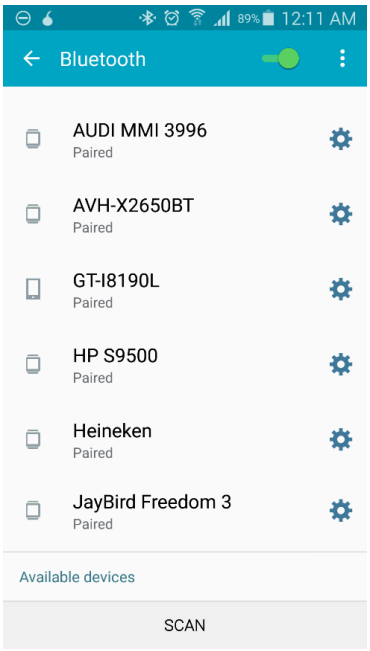



Figura 2.4: Dispositivos Bluetooth identificados por un nombre amigable al usuario

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.

#### 2.2.1.4. 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 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 solo 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.

#### 2.2.1.5. 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.

## 2.3. 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 [16, 17]. Posteriormente, en 1991, los miembros fundadores del CARO (Computer Antivirus Researchers Organization) Vesselin Bontchev, Fridrik Skulason y Alan Sólomon [18] 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 solo 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 [19].

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 miles de millones 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 mil millones de dólares en 2006 [20], mientras que

el Cibercrimen alcanzó un total estimado de forma conservadora de $375 mil millones de dólares en 2014 [21]. De aquí la importancia de su estudio y modelación.

### 2.3.1. Diferencias entre virus y gusanos

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

#### 2.3.1.1. 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 siempre y cuando, el usuario realice una acción que lo ejecute de forma consciente o inconsciente; por ejemplo, abrir una imagen infectada o montar un dispositivo removible como discos duros, memorias USB o MicroSD, donde el archivo *AUTORUN* este infectado.

#### 2.3.1.2. 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 interacción alguna del usuario. 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.

## 2.4. Propagación de gusanos en teléfonos inteligentes vía Bluetooth

Como se observó anteriormente, los tipos de malware que pueden ser encontrados es amplio, así como los medios por el cual puede ser propagado. Este trabajo de investigación se centra en el malware tipo gusano; el cual es propagado a través de antenas Bluetooh, al hacer copias de sí mismo y enviarlas a otros dispositivos en su proximidad sin la intervención o conocimiento del propietario del dispositivo.

Cuando un teléfono inteligente está infectado, 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 les permite ser descubribles, responderán a la solicitud de indagación, haciendo 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 enviará 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 entrará nuevamente en el estado de difusión del mensaje de indagación. Cuando el gusano es activado y en consecuencia, ejecutado en el dispositivo susceptible, se volverá infectado y entrará en la fase de difusión del mensaje de indagación para encontrar nuevos vecinos susceptibles. La figura 2.5 describe el proceso de propagación del gusano [3, 22].

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.

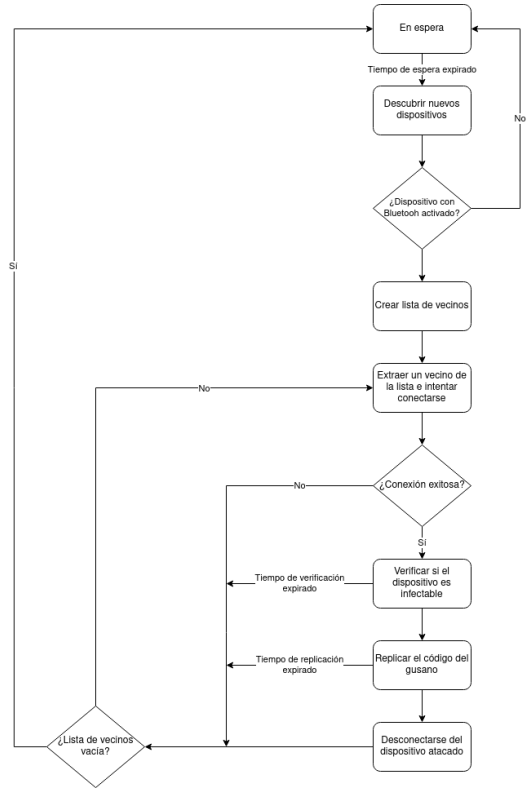



Figura 2.5: Ciclo de vida de Infección de un Gusano por Bluetooth

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.

Los primeros casos de malware transmitido a través de antenas Bluetooth data del 2004 con Cabir [23] y posteriormente, en 2005 con CommWarrior [24]. El método de propagación de Cabir fue muy original e inofensivo [25,26], el tiempo de vida del malware era corto y dependía de la proximidad de los dispositivos objetivo. Además, en 2004, menos del 2 % del mercado era ocupado por dispositivos con este tipo de antenas, lo que en consecuencia

hacía que los brotes a corto y mediano plazo fueran poco probables [27]. Finalmente, la tecnología Wi-Fi ofrecía un mecanismo de propagación incluso superior para el malware de móvil a móvil, ya que no requería autenticación, por lo que su tráfico era más fácil de rastrear y falsificar en comparación con el Bluetooth. Asimismo, la antena Wi-Fi siempre está encendida, a diferencia de la antena Bluetooth y, en general, en modo descubrible para ser explotada por el malware. Otra razón importante por la que las antenas Bluetooth no se consideraron un vector de ataque fue que las primeras versiones del estándar tenían muchos errores, problemas de comunicación y problemas de latencia, lo que hizo que la tecnología Bluetooth cayera en desuso durante muchos años. Durante este tiempo, los atacantes ignoraron Bluetooth y escribieron malware a través de otros vectores, tales como MMS, SMS y Wi-Fi, principalmente.

Muchos de los factores limitantes que hacían a los atacantes no considerar a las antenas Bluetooth han cambiado en los últimos años. Bluetooth ha resuelto muchos de los problemas de fiabilidad y rendimiento que solía tener. Al mismo tiempo, el número de dispositivos Bluetooth se ha disparado, y el número de aplicaciones y dispositivos que ahora utilizan este tipo de antenas no tiene precedentes (según la actualización del mercado de Bluetooth 2018, este año, el número de dispositivos habilitados con esta tecnología alcanzó los 4,000 millones [28]). Mientras que otros vectores de ataque, como Wi-Fi y actualmente las redes 4G-5G, siguen siendo formas más rápidas de atacar los dispositivos móviles, las antenas Bluetooth, por su gran número de aplicaciones y dispositivos, hacen de esta una tecnología que ya no puede considerarse libre de riesgos.

Dado que Bluetooth carece de una infraestructura de seguridad centralizada, los riesgos aumentan a medida que esta tecnología se extiende por todo el mundo. Por ello, en los últimos años se han producido graves vulnerabilidades de seguridad. Una de ellas es BlueBorne, un vector de ataque publicado recientemente que aprovechaba las brechas de seguridad en las conexiones clásicas de Bluetooth y que puede utilizarse para ejecutar código malicioso en los dispositivos afectados [29, 30]. BlueBorne no requería ninguna interacción con el usuario y solo necesitaba que la antena Bluetooth estuviera encendida. Recientemente, en 2020, la vulnerabilidad de seguridad BlueFrag permitió la ejecución de código a través de Bluetooth en algunos dispositivos Android [31]. En BlueFrag, un atacante remoto podía ejecutar código arbitrario de forma silenciosa, con los privilegios del demonio Bluetooth y sin requerir ninguna interacción del propietario del dispositivo. Para que BlueFrag funcionara, era necesario conocer la dirección MAC de la ante-

na Bluetooth del dispositivo objetivo, que en la mayoría de los casos puede deducirse de la dirección MAC de la antena Wi-Fi. Por otro lado, a partir de 2016, cuando se lanzó la versión 5 de Bluetooth, se consiguió aumentar la capacidad de transmisión ocho veces y el alcance hasta 200 m (en exteriores) o 40 m (en interiores). Esta versión fomentó ampliamente el uso de la tecnología Bluetooth, especialmente para el IoT. Recientemente, derivado de la pandemia de COVID-19, muchos gobiernos y empresas están pensando en formas de contener la pandemia utilizando Bluetooth a través de las llamadas apps de seguimiento del SARS-CoV-2. Estas apps ya se utilizan ampliamente en algunos países, como India, Singapur y Australia [32–39]. Las aplicaciones de monitoreo de COVID-19 requieren que la antena Bluetooth esté siempre activada, lo que resulta atractivo para los desarrolladores de malware.

Por lo anterior, es posible que en los próximos años se propaguen nuevos programas maliciosos a través de Bluetooth y en consecuencia, es de suma importancia analizar y comprender la propagación de los programas maliciosos. Sin duda, para luchar contra éste tipo de amenazas propagadas por antenas Bluetooth es esencial disponer de métodos eficaces para detectar los tipos de programas maliciosos. Además, los modelos matemáticos y computacionales son herramientas poderosas para entender la propagación del malware y explorar el impacto de varios parámetros en diferentes escenarios. Sin embargo, estos modelos deben reflejar la realidad de la mejor manera posible. Aunque los modelos no pueden responder a todas las preguntas, el contar con modelos matemáticos que describan y analicen la propagación de malware tipo gusano en teléfonos inteligentes proporcionarán indicios que pueden ayudar a resolver el rompecabezas para comprender mejor y reevaluar la probabilidad de infección de malware, incluso en entornos concurridos [40].

Por otra parte, dado que la investigación que se presenta en este trabajo de tesis se basa en el uso del paradigma de Autómatas Celulares (AC), en la siguiente sección se introduce brevemente el mismo.

## 2.5. 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 posibi-

lidad de crear máquinas que a su vez pudieran crear máquinas más complejas que ella. Von Neumann observó que, de manera análoga a los procesos biológicos, las células pueden generar construcciones más complejas. Así, el concepto de complejidad en las máquinas puede ser basado en la idea de la auto-reproducción [41].

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 en la figura 2.6. Ésta es 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.

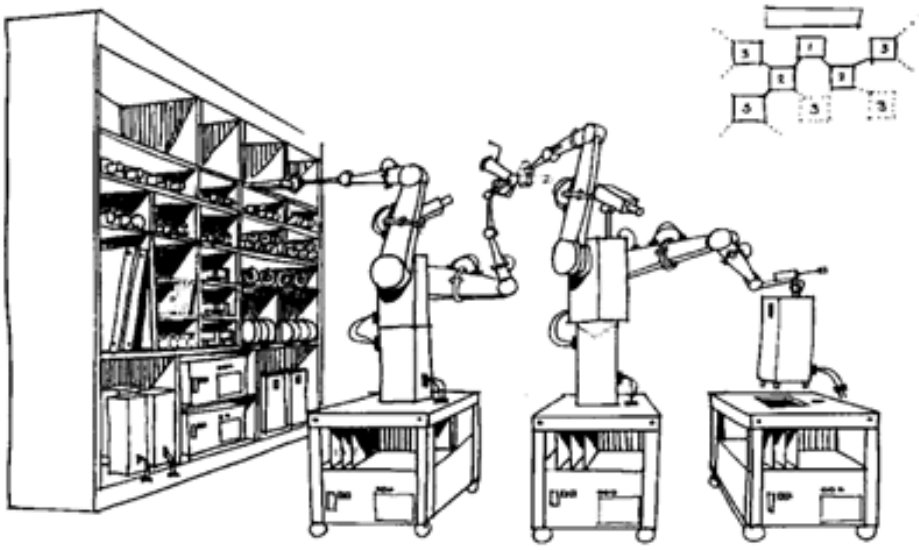


Figura 2.6: Demostración propuesta del robot simple de auto-replicación. Título original en inglés: "Proposed demonstration of simple robot self-replication", por la NASA Conference Publication 2255 (1982)

La modelación de esta máquina auto-replicable como un 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 autoreplicable es un AC bidimensional.

En términos generales, los AC son sistemas dinámicos discretos, cuyo espacio y tiempo son discretos; y por lo tanto, también lo son las variables de estado que lo describen. 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 $(C, \Sigma, V, f)$, donde $C$ representa el espacio celular, $\Sigma$ 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 [42].

Los AC están compuestos por los siguientes elementos que los definen:

- 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 figura 2.7 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 solo 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 determinista y da el estado $Si(t+1)$ de la i-ésima célula en el paso de tiempo $t+1$ en función del estado de las células en el vecindario.

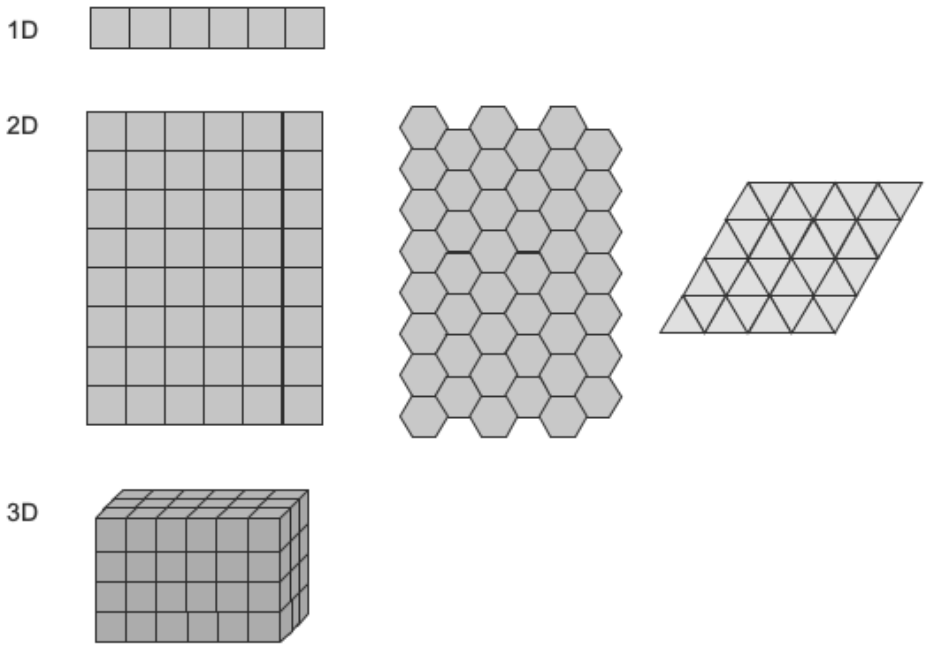



Figura 2.7: Espacios Celulares de los AC.

- 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 figura 2.8.

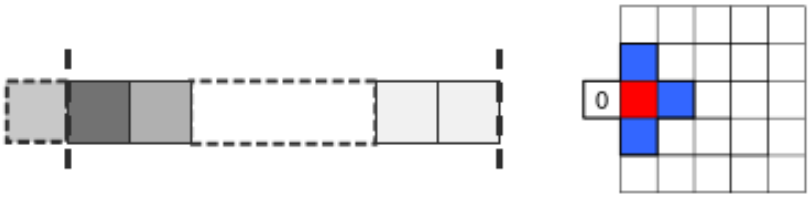



Figura 2.8: Frontera asignada

- 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 figura 2.9:

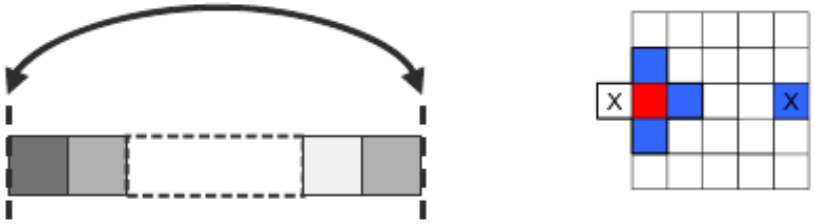



Figura 2.9: Frontera periódica

- 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 figura 2.10.

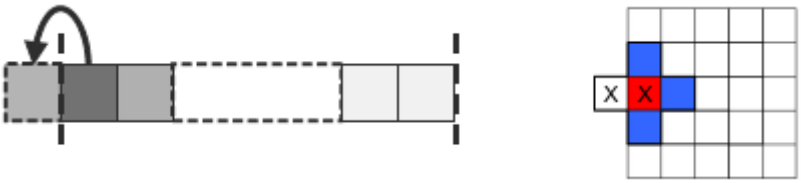



Figura 2.10: Frontera Adiabática

- 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 figura 2.11 ilustra el concepto:

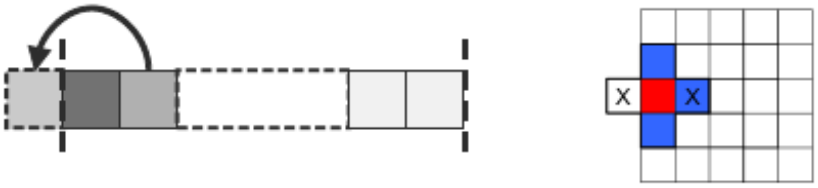



Figura 2.11: Frontera de Reflexión

- 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 figura 2.12.

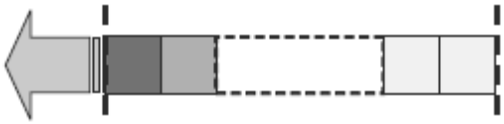


Figura 2.12: Frontera de Absorción

•

Debido a que los gusanos Bluetooth atacan e infectan a los dispositivos que se encuentran en su proximidad, la propagación del malware muestra una gran similitud con el comportamiento de auto-replicación y propagación de los virus biológicos. En consecuencia, un enfoque común para modelar este comportamiento es utilizar las teorías clásicas de propagación de la epidemiología. 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 epidemiológicos compartimentales, principales modelos de propagación de malware existentes y sus características.

# 3

# Una breve revisión de los modelos de Malware

En este capítulo, se presenta una breve introducción a los conceptos de modelos epidemiológicos compartimentales y descripción del estado del arte con relación a los mismos en los últimos años.

La aplicación de las matemáticas a la epidemiología 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 a 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, ha llegado a ser 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.

## 3.1. 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 [43].

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.

## 3.2. Modelos epidemiológicos genéricos

La modelación epidemiológica tiene una larga historia en el estudio de las enfermedades biológicas infecciosas. En 1927 [44], 1932 [45] y 1933 [46], Kermack y McKendrick publicaron una serie de artículos titulados *"Contributions to the mathematical theory of epidemics"*. Dichos artículos son vistos

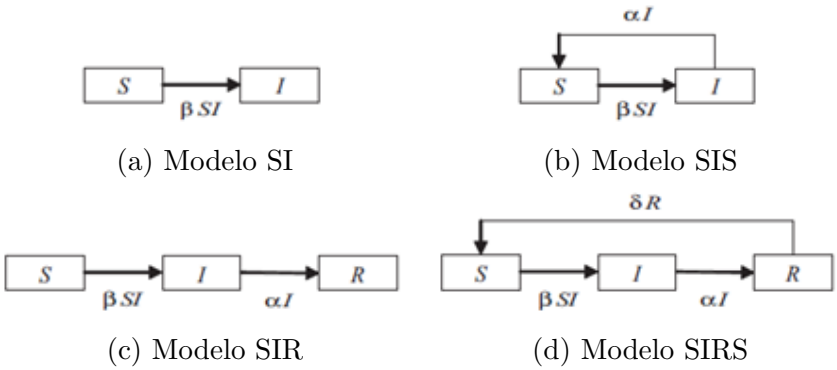
como la base para más investigaciones empleando el modelado matemático (especialmente el determinístico) para explorar la propagación de las enfermedades infecciosas. Los modelos epidemiológicos clásicos incluyen el modelo SI (Susceptible-Infectado), el modelo SIS (Susceptible-Infectado-Susceptible), y el modelo SIR (Susceptible-Infectado-Recuperado) [47].

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. Comúnmente, en este tipo de modelos epidemiológicos, el tamaño total de la población se considera constante.

Dentro de los modelos de este tipo se encuentran también los nombrados SI, SIS, SIR y SIRS, donde los individuos de la población son clasificados de acuerdo al estado de su enfermedad. Estos modelos en su forma básica son mostrados en las figuras 3.1a, 3.1b, 3.1c y 3.1d.

Algunos de los términos para estos modelos se explican a continuación:

- $\mu$ 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.
- $\lambda$ 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 ésta.
- *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.




(a) Modelo SI (b) Modelo SIS

(c) Modelo SIR (d) Modelo SIRS

Figura 3.1: Modelos Epidemiológicos Determinísticos Básicos

- *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.
- $\beta$ 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.
- $\alpha$ representa la tasa media de recuperación.
- $\delta$ 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.
- $\beta SI$ representa el número de nuevas infecciones por unidad de tiempo.
- $\alpha I$ representa el número de nuevas recuperaciones o denota el número de nuevos individuos susceptibles por unidad de tiempo.
- $\delta R$ representa el número de nuevos individuos susceptibles por unidad de tiempo.

En el modelo SI (Fig. 3.1a), 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. 3.1b), 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. 3.1c), 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. 3.1d), se asume que los individuos infectados pueden recuperarse y nuevamente volverse susceptibles tras la recuperación.

## 3.3. 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 mencionó anteriormente, la mayoría de los modelos epidemiológicos existentes están basados en el modelo Kermack-McKendric y pueden ser agrupados en tres grandes categorías [47]: 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 las principales desventajas de este tipo de modelos 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. Además, en este tipo de modelos se ha observado 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.

Por otra parte, en los modelos estocásticos [47], 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, el análisis matemático suele ser complicado.

Los modelos espacio-temporales [47] 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 3.1 se resume un comparativo de las características de los modelos epidemiológicos de propagación.

## 3.4. Los modelos basados en Autómatas Celulares

De forma análoga a las enfermedades biológicas infecciosas, el modelado de las interacciones entre individuos refleja un comportamiento más detallado que se asemeja mejor a los escenarios de la vida real. En este sentido, los modelos basados en autómatas celulares (AC) se han convertido en una alternativa bien establecida para simular, analizar y comprender el comportamiento y la propagación de los gusanos [48–54]. Como se definió en el capítulo anterior, los AC son sistemas dinámicos en tiempo discreto donde los individuos interactúan en un espacio celular [55], cuyo estado también es discreto. El estado de cada uno de los individuos se actualiza en paralelo en cada paso de tiempo discreto, siguiendo un sencillo conjunto de reglas homogéneas. Cuando este conjunto de reglas induce procesos estocásticos, el AC puede considerarse un paradigma de un gran sistema dinámico en el que se permite que muchas partículas interactúen bajo ciertas reglas locales de vecindad. De este modo, los nuevos estados individuales se eligen de acuerdo

| 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 |

Cuadro 3.1: Modelos básicos para dinámica de propagación

con algunas distribuciones de probabilidad. Por lo tanto, el comportamiento del sistema completo depende de la naturaleza de la interacción entre los individuos. Así, las AC pueden considerarse cadenas de Markov que interactúan localmente, en los que es teóricamente posible unir todos los individuos del espacio celular y proponer un sistema dinámico de muy alta dimensión, cuya estructura cambia drásticamente con el tiempo de forma no lineal para representar todas las interacciones factibles entre los individuos.

Peng et al. [48, 52] propusieron un modelo de AC para simular la dinámica de propagación de gusanos en redes Bluetooth basado en la consideración del grado de propagación de los nodos infectados y la resistencia hacia los nodos susceptibles. En 2015, Del Rey et al. [54] introdujeron un modelo CA cuya dinámica se basa en funciones de transición lógica. Este modelo consideraba la movilidad de los smartphones y la heterogeneidad de los sistemas operativos. Sin embargo, no consideraba algunos escenarios importantes para la propagación de gusanos por Bluetooth, como la interrupción de la transmisión de gusanos debido a la movilidad, ya que los dispositivos entran y salen del alcance de los demás. González et al. [56] propusieron un modelo bidimensional basado en CA para estudiar la propagación de un gusano Bluetooth basado en modelos epidemiológicos compartimentales. Dicha investigación clasificó cada estado epidémico del smartphone en uno de los siete tipos: susceptible, expuesto, infectado, diagnosticado, portador, interrumpido y recuperado. Definió un conjunto de reglas locales para simular la dinámica del modelo cuando se consideraban smartphones homogéneos. Recientemente, este modelo se amplió para considerar la probabilidad de recuperación al tener una actualización del antivirus y sus efectos contra el gusano. Sin embargo, los modelos descritos no tienen en cuenta otros factores que afectan a la propagación del gusano, como el comportamiento humano, la interacción con el usuario, las características de transmisión del malware y su impacto en la dinámica de propagación para determinar cómo podría propagarse un malware Bluetooth en diferentes condiciones. Esta investigación también considera diferentes rangos de transmisión debido a varios tipos de antenas Bluetooth, es decir, con un rango de transmisión de 1, 10 ó 100 m, así como la aceptación de la transmisión y el modo descubrible en función de la intervención directa del usuario.

En este trabajo de investigación, se amplía el modelo propuesto en [12] añadiendo las reglas necesarias para incluir nuevas características que permitan representar de mejor manera las interacciones y comunicaciones reales de los smartphones. Se consideran las siguientes características en la definición

de la dinámica del modelo propuesto y su comportamiento: 1) Distintas clases de antenas Bluetooth que, en consecuencia, implican diferentes alcances y velocidades de transmisión que afectan al tiempo de transmisión de la carga útil del gusano; es decir, un gusano puede propagarse más rápido en algunos dispositivos; 2) Factores de renovación para simular que los dispositivos existentes se mueven fuera del área de estudio y que los nuevos dispositivos se ingresan a ella; 3) La influencia de diferentes tipos de movilidad de los dispositivos. Además, el ajuste de los parámetros de entrada, por ejemplo, las tasas de transmisión, el tamaño de los archivos de los gusanos, etc., se realiza utilizando datos reales proporcionados por algunos informes públicos sobre software antivirus. El modelo propuesto es útil para representar la propagación de malware basado en vulnerabilidades del sistema operativo, cuya aparición es difícil de predecir. El gran número de dispositivos Bluetooth en circulación hace que el estudio de la propagación de malware sea un fenómeno relevante a analizar. De igual forma, se diseñaron diferentes escenarios de simulación para analizar cómo podría propagarse un gusano Bluetooth. Los experimentos tuvieron en cuenta el lugar donde se inicia el brote, la conciencia del usuario sobre los riesgos inherentes al uso de dispositivos inteligentes en redes Bluetooth y los diferentes tipos de antenas integradas en los dispositivos inteligentes. Los resultados de la simulación indican que el modelo propuesto es adecuado para estudiar cómo la demografía del usuario afecta a la propagación del gusano en el tiempo y el espacio.

Una vez introducidos los conceptos fundamentales empleados en este trabajo y el estado del arte, en el siguiente capítulo se presenta el modelo propuesto.

# 4

# Un modelo de la dinámica espacio-temporal de la propagación de malware a través de Bluetooth considerando el comportamiento humano

En este capítulo, se presenta un nuevo modelo matemático basado en AC el cual toma en cuenta las características individuales de los dispositivos desplegados en el espacio celular, así como algunas características importantes, tales como, interrupción de la infección por cuestiones de movilidad de los dispositivos, interacciones del usuario, distintos patrones de movimiento, entre otros; que tienen una incidencia directa y determinante en la mecánica de propagación del gusano.

Como se mencionó, los autómatas celulares (AC) son un paradigma de modelado intuitivo para los sistemas complejos. Los AC son modelos matemáticos de sistemas dinámicos, espacial y temporalmente discretos. Están compuestos por un conjunto finito de células, cada una de las cuales puede estar ocupada por agentes que evolucionan en paralelo en pasos de tiempo discretos. El estado de cada agente se actualiza de acuerdo con un conjunto de reglas de transición dinámicas que tienen en cuenta el estado de los agentes en las células de su vecindad.

Formalmente, un AC puede definirse como una tupla de cinco, $\{N, \mathcal{C}, \Omega, V, f\}$, donde $N$ es el conjunto de agentes individuales, $\mathcal{C}$ denota el espacio celular, $\Omega$ denota un conjunto de estados finito cuyos elementos son todos los estados posibles de los agentes, $V$ denota la vecindad de celdas de cada agente, y $f$ denota un conjunto de reglas de transición local. En particular, para los AC

bidimensionales, el espacio celular $\mathcal{C}$ se representa como un entramado espacial regular o rejilla $\mathcal{C}$ de $L \times M$ células, $\mathcal{C} = \{(i,j) \mid i,j \in Z, 1 \leq i \leq L, 1 \leq j \leq M\}$. En el momento $t$, cada agente permanece en uno de los números finitos de posibles estados discretos en $\Omega$. Al interactuar con los agentes de su vecindario $V$, cada agente actualiza su estado actual siguiendo el conjunto de reglas de transición específicas en $f$.

## 4.1. El modelo propuesto

El modelo propuesto es un autómata celular probabilístico basado en agentes. Los agentes son $N$ individuos con smartphones desplegados aleatoriamente en la cuadrícula bidimensional $C$, que representa el área geográfica en estudio. Así, cada celda tiene una posición asociada $(i,j)$, que en este trabajo representa un área de 1 $m^2$. Además, las celdas pueden estar vacías u ocupadas por un solo individuo con un smartphone, como se muestra en la Fig. 4.1a. Las transiciones en el tiempo van desde $t \to t+1$, lo que implica que el paso de tiempo es igual a 1s.

Por otro lado, cada smartphone $u \in N$ en la posición $(i,j)$ puede establecer contacto solo con aquellos smartphones dentro de una vecindad $V(u)_{(i,j)}$ que representa el rango de transmisión radial de una antena Bluetooth utilizando una vecindad de Moore bidimensional con radio $r$, cuyo valor depende de la clase de antena Bluetooth considerada y que se define por:

$$V(u)_{(i,j)} = \{(x,y) : |x-i| <= r, |y-j| <= r\}$$

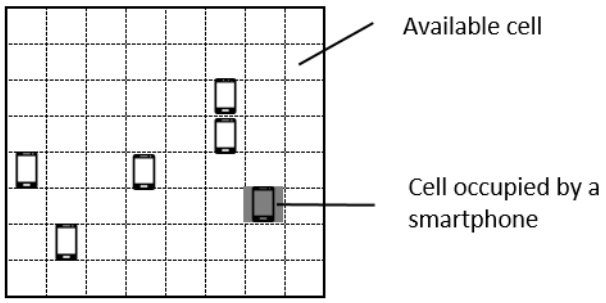
como se muestra en la figura 4.1b.

En este modelo, solo se consideran dos clases de antena Bluetooth, que se describen en [57]: clase 2 (10 m de alcance de transmisión) y clase 3 (1 m de alcance de transmisión).

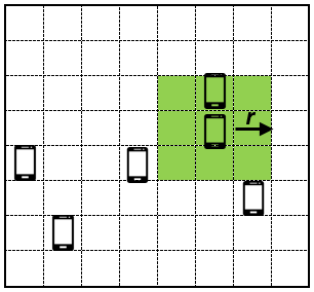
### 4.1.1. Estados de los smartphones

El estado epidémico de un smartphone se divide según la dinámica de propagación de los gusanos Bluetooth de la siguiente manera:

a. **Estado susceptible (S)**. Indica los dispositivos que no han sido infectados por otro smartphone infeccioso pero que son propensos a la infección.




(a) Representación discretizada del espacio geográfico y el posicionamiento de un smartphone.




(b) Modelación del rango de la antena Bluetooth empleando una vecindad de Moore.

Figura 4.1: Espacio celular $\mathcal{C}$

b. **Estado expuesto (E)**. Dispositivos que han estado en contacto con el gusano, pero que aún no pueden contagiar a un smartphone susceptible porque todavía no se les ha transmitido una copia completa del gusano.

c. **Estado infectado (I)**. Dispositivos que han recibido una copia completa de un gusano compatible con su sistema operativo. Por lo tanto, pueden infectar a otros smartphones susceptibles dentro de su rango de transmisión.

d. **Estado de portador (C)**. Dispositivos que han recibido una copia completa de la carga útil del gusano que no es compatible con su sistema operativo. En consecuencia, se asume que el gusano no puede funcionar correctamente y no es capaz de seguir propagándose. Este es un estado terminal.

e. **Estado recuperado (R)**. Dispositivos en los que se ha eliminado el gusano aplicando una restauración de fábrica o restaurando una copia de seguridad, lo que les confiere inmunidad temporal. Los dispositivos en un estado Recuperado pueden volver a un estado Susceptible, lo que representa que algunos dispositivos salen del espacio celular y otros nuevos entran, manteniendo así el número total $N$ constante.

f. **Estado interrumpido (INT)**. Denota los dispositivos expuestos que

reciben una copia del gusano y que, debido a su movilidad, salieron del rango de transmisión del dispositivo infectado antes de que terminara la transmisión de la carga útil del gusano. Este estado también engloba a los dispositivos que reciben una copia del gusano y la recuperación del correspondiente smartphone infectado. Un dispositivo que haya alcanzado este estado volverá al estado Susceptible en el siguiente paso de tiempo.

El estado de infección para el smartphone $u$ situado en la posición $(i, j)$, en el paso de tiempo $t$ se denota por $\omega_{ij}^{u}(t)$, en el que $\omega_{ij}^{u}(t) \in \{\text{S,E,C,I,R,INT}\}$.

Sea el número de dispositivos susceptibles, expuestos, portadores, infecciosos y recuperados en el momento $t$ denotado por $S(t)$, $E(t)$, $C(t)$, $I(t)$, $R(t)$ e $INT(t)$, respectivamente. Entonces, $N = S(t) + E(t) + C(t) + I(t) + R(t) + INT(t)$, lo que implica que $N$, el número de smartphones en el espacio celular $\mathcal{C}$ permanece constante durante todo el tiempo de simulación.

### 4.1.2. Atributos de los smartphones

Cada agente en el espacio celular $\mathcal{C}$ es un smartphone provisto de atributos que corresponden a dispositivos reales, cuyo valor se almacena en las variables individuales descritas en la tabla 4.1. Inicialmente, los smartphones se despliegan aleatoriamente en el espacio celular con una probabilidad $P_{MOV}$ de empezar a moverse aleatoriamente. En cada paso de tiempo, un smartphone puede moverse desde su posición actual $(i, j)$ a cualquier celda adyacente disponible en su vecindad.

### 4.1.3. Transición de estados

Para describir las fases de propagación del gusano a través de las antenas Bluetooth, el modelo considera las siguientes reglas para controlar su evolución:

a. **Del estado susceptible a expuesto**. Esta transición representa la situación en la que el propietario de un smartphone sano acepta la transmisión de un smartphone infectado en su vecindario, lo que indica que la infección puede comenzar. Para que esto ocurra, deben cumplirse cuatro condiciones 1) La probabilidad de infección por un smartphone infeccioso cercano; 2) La antena Bluetooth debe estar encendida; 3) La antena debe estar en modo descubrible; y 4) El usuario debe aceptar la transmisión entrante.

Cuadro 4.1: Atributos de un agente de smartphone $u$ en el tiempo $t$

| Atributo | Descripción |
|---|---|
| os | Tipo de sistema operativo instalado (Android u otro) |
| $\omega_{ij}^{u}(t)$ | Estado actual del smartphone en el tiempo $t$. Las funciones de transición emplearan este valor para calcular el estado siguiente |
| $\omega_{ij}^{u}(t+1)$ | Estado al cual un smartphone transicionará al siguiente paso de tiempo $t+1$ |
| IST | Tiempo de inicio de infección. Paso de tiempo en el que un smartphone pasó al estado E. El valor de este atributo será considerado en $t+1$, ya que la conexión entrante debe ser aceptada antes de iniciar la transmisión |
| $\mathrm{U}_{u_{\mathrm{BT}}}^{t}$ | Variable lógica que indica si la antena Bluetooth está encendida |
| $\mathrm{D}_{u}^{t}$ | Variable lógica que indica si la antena Bluetooth esta en modo descubrible |
| $\mathrm{A}_{u_{acc\_v}}^{t}$ | Variable lógica que indica si el dueño del smartphone acepta la transmisión entrante de un dispositivo vecino $v$ en el tiempo $t$ |

En consecuencia, la función lógica utilizada para determinar la transición de un estado Susceptible a uno Expuesto se describe de la siguiente forma:

$$f_{T_{SE}}(u) = \mathrm{X}_{p_i}^{t} \wedge \mathrm{U}_{u_{\mathrm{BT}}}^{t} \wedge \mathrm{D}_{u}^{t} \wedge \mathrm{A}_{u_{acc\_v}}^{t} \tag{4.1}$$

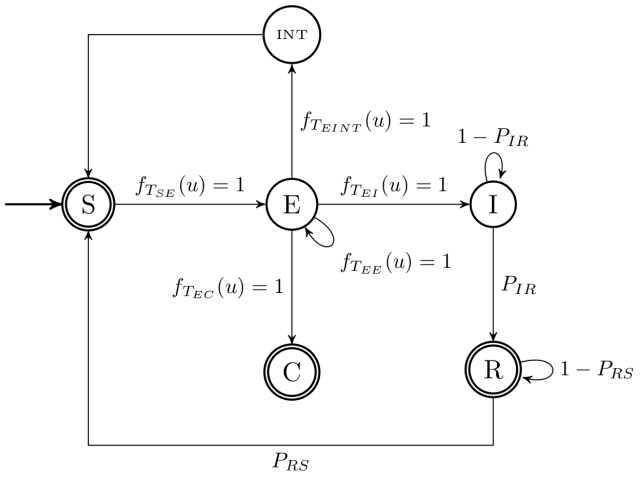



Figura 4.2: Diagrama de transición de estados de un smartphone arbitrario

con

$$\mathrm{X}^t_{p_i} = \begin{cases} 1 & \text{con probabilidad } P_{Contagion} = \beta \frac{I_u(t)}{N_u(t)} \\ 0 & \text{con probabilidad } 1 - P_{Contagion} \end{cases} \tag{4.2}$$

$$\mathrm{U}^t_{u_{\mathrm{BT}}} = \begin{cases} 1 & \text{con probabilidad } P_{BT} \\ 0 & \text{con probabilidad } 1 - P_{BT} \end{cases} \tag{4.3}$$

$$\mathrm{D}^t_u = \begin{cases} 1 & \text{con probabilidad } P_D \\ 0 & \text{con probabilidad } 1 - P_D \end{cases} \tag{4.4}$$

$$\mathrm{A}^t_{u_{acc\_v}} = \begin{cases} 1 & \text{con probabilidad } P_{acc} \\ 0 & \text{con probabilidad } 1 - P_{acc} \end{cases} \tag{4.5}$$

donde $u \in N$ es el smartphone en la ubicación de la celda $(i, j)$, $N_u(t)$ es el número total de smartphones vecinos de $u$ en el tiempo $t$, $\beta \in [0, 1]$ es la tasa de infección, con base en [44], y $I_u(t)$ es el número total de smartphones infectados en la vecindad de $u$ en el tiempo $t$. Así, $\mathrm{X}^t_{p_i}$ es la variable lógica que indica si un smartphone podría estar infectado por un gusano transmitido por un smartphone infeccioso cercano. $\mathrm{U}^t_{u_{\mathrm{BT}}}$ es una variable lógica que indica si la antena del smartphone $u$ está encendida en el momento $t$ con probabilidad $P_{BT}$. $\mathrm{D}^t_u$ indica si la antena del smartphone $u$ está en modo descubrible en el momento $t$ con una probabilidad $P_D$.

Por último, $A^t_{u_{acc\_v}}$ también toma un valor lógico que indica si el propietario del smartphone $u$ acepta la transmisión entrante de un smartphone vecino $v$ en el tiempo $t$ con una probabilidad $P_{acc}$. En consecuencia, la transición de un estado Susceptible a uno Expuesto se da de la siguiente manera:

$$\omega^u_{ij}(t+1) = \begin{cases} \text{E}, & \omega^u_{ij}(t) = \text{S}, f_{T_{SE}}(u) = 1 \\ \text{S}, & \omega^u_{ij}(t) = \text{S}, f_{T_{SE}}(u) = 0 \end{cases} \tag{4.6}$$

b. **Del estado expuesto a infectado, o de expuesto a interrumpido, o de expuesto a portador**. Esta transición de estado representa lo que le ocurre a un smartphone expuesto que ya está en contacto con uno infectado. Pueden ocurrir tres eventos posibles: 1) Los smartphones expuestos e infectados permanecen en el rango de transmisión $r$ durante un tiempo de latencia $LT$ hasta que se envía el gusano y ambos dispositivos tienen el mismo sistema operativo; 2) Los smartphones expuestos e infectados interrumpen la transmisión saliendo del rango $r$ antes de que se complete el tiempo de latencia $LT$; y 3) El smartphone infectado completa la transmisión del gusano en el tiempo $LT$, sin embargo, el smartphone receptor tiene un sistema operativo diferente al del objetivo del gusano. Para aclarar esta transición, supongamos que en el tiempo $t$ la célula $(i, j)$ está ocupada por el smartphone de interés $u$ con el estado actual $E$ denotado como $\omega^u_{ij}(t) = \text{E}$ que evolucionará en el tiempo $t+1$ al estado C, I o INT según las siguientes condiciones:

$$\omega^u_{ij}(t+1) = \begin{cases} \text{E}, & \omega^u_{ij}(t) = \text{E}, f_{T_{EE}}(u) = 1 \\ \text{INT}, & \omega^u_{ij}(t) = \text{E}, f_{T_{EINT}}(u) = 1 \\ \text{I}, & \omega^u_{ij}(t) = \text{E}, f_{T_{EI}}(u) = 1 \\ \text{C}, & \omega^u_{ij}(t) = \text{E}, f_{T_{EC}}(u) = 1 \end{cases} \tag{4.7}$$

donde $f_{T_{EE}}(u)$, $f_{T_{EINT}}(u)$, $f_{T_{EI}}(u)$ y $f_{T_{EC}}(u)$ son funciones lógicas que un smartphone utiliza para cambiar su estado desde el estado E definido como sigue:

Cuadro 4.2: Ejemplo de los atributos de un smartphone expuesto

| Smartphone $u$ | | |
|---|---|---|
|  | osType | Android |
| | Estado actual | Expuesto |
| | IST | 10 |

| Smartphone $u'$ | | |
|---|---|---|
|  | osType | Android |
| | Estado actual | Expuesto |
| | IST | 14 |

$$f_{T_{EE}}(u) = \begin{cases} 1 & t < \Delta t \wedge v_I \in V_u \\ 0 & \text{en caso contrario} \end{cases} \tag{4.8}$$

$$f_{T_{EINT}}(u) = \begin{cases} 1 & t < \Delta t \wedge (v_I \notin V_u \vee U^t_{BT_u} = 0) \\ 0 & \text{en caso contrario} \end{cases} \tag{4.9}$$

$$f_{T_{EI}}(u) = \begin{cases} 1 & t \geq \Delta t \wedge v_I \in V_u \wedge u_{os} = v_{I_{os}} \\ 0 & \text{en caso contrario} \end{cases} \tag{4.10}$$

$$f_{T_{EC}}(u) = \begin{cases} 1 & t \geq \Delta t \wedge v_I \in V_u \wedge u_{os} \neq v_{I_{os}} \\ 0 & \text{en caso contrario} \end{cases} \tag{4.11}$$

Aquí, $V_u$ representa la vecindad del smartphone $u$. $v_I \in V_u$ denota el dispositivo infectado que está transmitiendo el gusano al smartphone $u$ en el paso de tiempo $t$. $u_{os}$ y $v_{I_{os}}$ se utilizan para denotar el tipo de sistema operativo del smartphone de los dispositivos $u$ y $v_I$, respectivamente. $\Delta t$ representa el tiempo necesario para que se complete la infección, definido como $\Delta t = IST + \text{LT}$; en el que $IST$ representa la hora de inicio de la infección y LT el tiempo de latencia.

Para ilustrar este caso, consideremos dos smartphones diferentes denominados $u$ y $u'$, respectivamente, cuyos atributos se muestran en la tabla 4.2. Supongamos que ambos smartphones aceptan la transmisión del gusano de un smartphone infectado en su vecindario y cambian del estado Susceptible a Expuesto en el tiempo $t = 10$ y $t = 14$, respectivamente. La figura 4.3 representa su evolución en el tiempo, en la que se puede observar que los smartphones $u$ y $u'$ se infectan en el tiempo $t = 17$ s y $t = 21$ s, respectivamente.

c. **Del estado interrumpido a susceptible**. Esta transición de estado representa la situación en la que un smartphone estaba conectado a un

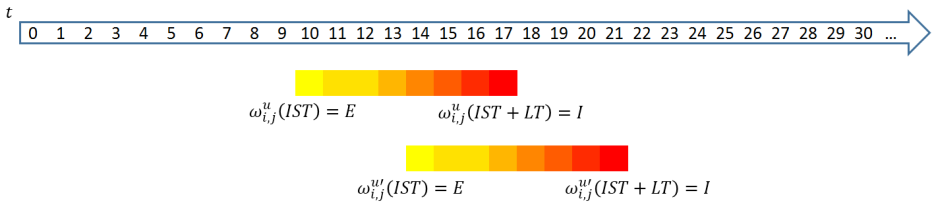



Figura 4.3: Línea de tiempo en la transición del estado expuesto al infectado, asumiendo un tiempo de latencia $LT = 7$ s

dispositivo infectado y uno de los dos dispositivos salió del alcance de la antena Bluetooth antes de que la transmisión del gusano terminara. Por lo tanto, se asume que la conexión fue interrumpida. En consecuencia, el smartphone expuesto no tiene una copia completa del gusano, por lo que no se ve afectado por él y, por tanto, vuelve a un estado Susceptible. Suponiendo que el smartphone $u$ se encuentra en la célula $(i, j)$ y su estado actual es $INT$ denotado como $\omega^{u}_{ij}(t) = \text{INT}$, entonces el estado evolucionará incondicionalmente al estado $S$ al siguiente paso de tiempo, como se muestra en la ecuación (4.12).

$$\omega^{u}_{ij}(t+1) = \text{S} \tag{4.12}$$

d. **Del estado infectado a recuperado**. Esta transición de estado representa el intento del propietario de un smartphone infectado de recuperar su dispositivo mediante la restauración de una copia de seguridad o un reinicio de fábrica. Suponiendo que el smartphone $u$ se encuentra en la celda $(i, j)$ y su estado actual es I, denotado como $\omega^{u}_{ij}(t) = \text{I}$; éste evolucionará al estado R si se cumple la probabilidad $P_{IR}$ se cumple, lo que indica que el intento de eliminar el gusano del sistema operativo tuvo éxito; en caso contrario, el dispositivo permanecerá en el estado I. La transición se produce de la siguiente manera:

$$\omega^{u}_{ij}(t+1) = \begin{cases} \text{R}, & \omega^{u}_{ij}(t) = \text{I con probabilidad } P_{IR} \\ \text{I}, & \omega^{u}_{ij}(t) = \text{I con probabilidad } 1 - P_{IR} \end{cases} \tag{4.13}$$

### 4.1.4. Dinámica de movilidad

El modelo propuesto introduce la movilidad de los smartphones por el espacio celular $\mathcal{C}$, un factor importante en el proceso de infección por Bluetooth. Así, cada smartphone puede moverse a una de las celdas disponibles más cercanas en un vecindario de Moore en cada paso de tiempo, siempre que se cumpla la probabilidad de movimiento $P_{MOV}$, como se muestra en la figura 4.4. Se consideran tres tipos diferentes de movimientos:

a. Línea Recta (SL). Un smartphone continuará moviéndose en la misma dirección con probabilidad $P_{MOV}$ si y solo si otro smartphone no esta ocupando la célula de destino o la célula destino se encuentra en el límite del espacio celular. En caso contrario, el smartphone permanecerá en su celda de origen, y se le asignará una nueva dirección en el siguiente paso de tiempo (ver figura 4.5a).

b. Caminata Aleatoria (RW). Un smartphone se moverá en una dirección seleccionada aleatoriamente en cada paso de tiempo con una probabilidad $P_{MOV}$ si, y solo si, otro smartphone no está ocupando la célula de destino o la célula destino se encuentra en el límite del espacio celular. En caso contrario, el smartphone permanecerá inmóvil (ver figura 4.5b).

c. Movimiento Mixto con Pausas (MMwP). Un smartphone se moverá con una probabilidad $P_{MOV}$, según los siguientes pasos:

   *a*) Asignar una ventana de tiempo con una duración entre [1,5] segundos.

   *b*) Asignar un patrón de movimiento (SL, RW o una pausa).

   *c*) Ejecutar el movimiento, empleando la ventana de tiempo y el patrón asignados.

   *d*) Repetir los tres primeros pasos hasta finalizar la simulación.

   Este movimiento se muestra en la figura 4.5c.

La tabla 4.3 contiene un resumen de los parámetros del modelo propuesto.

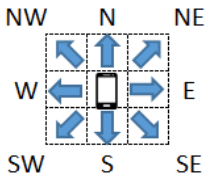
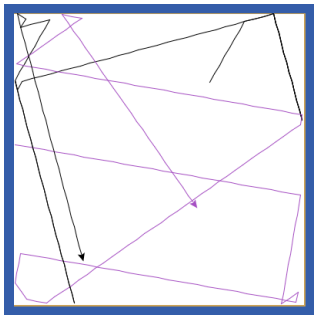
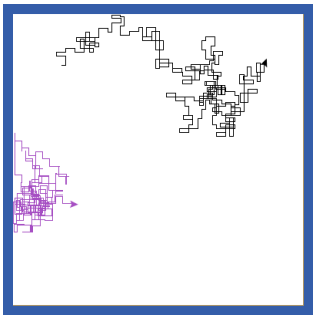


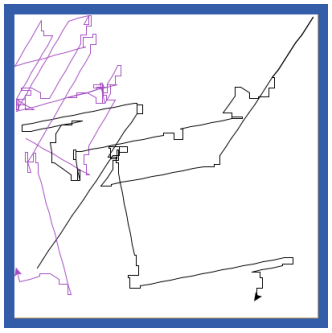

Figura 4.4: Uso de una vecindad de Moore para asignar una dirección de movimiento para los smartphones



(a) Línea Recta.



(b) Caminata Aleatoria.



(c) Movimiento Mixto con Pausas.

Figura 4.5: Primeros 200 pasos de tiempo de de dos smartphones empleando los tres distintos modelos de movimiento. La punta de la flecha indica la dirección del movimiento.

Cuadro 4.3: Parámetros y variables generales de entrada.

| Parámetro | Descripción |
|---|---|
| $\beta$ | Tasa de infección |
| LT | Tiempo de latencia |
| $P_{MOV}$ | Probabilidad de movimiento |
| $P_{IR}$ | Probabilidad de recuperar un smartphone infectado |
| $P_{RS}$ | Probabilidad de que un smartphone recuperado evoluciones al estado Susceptible |
| $P_{BT}$ | Probabilidad de que la antena del smartphone esté encendida en el tiempo $t$ |
| $P_{acc}$ | Probabilidad de que un smartphone acepte la transmisión del gusano de un dispositivo infectado en el tiempo $t$ |
| $P_D$ | Probabilidad de que un smartphone esté en modo descubrible en el tiempo $t$ |

### 4.1.5. Consideraciones generales del modelo propuesto

- Este modelo considera las conexiones Bluetooth como un vector de infección solamente. La pila de Bluetooth y otras características de bajo nivel están fuera del alcance de está investigación.
- Los smartphones pueden tener diferentes características o configuraciones, que influyen en la forma de propagación del gusano (sistemas operativos y configuraciones de seguridad).
- Los sistemas operativos considerados en este modelo son Android y otros (iOS, Windows, etc.)
- La dinámica de infección considera que un smartphone infectado puede atacar a otros susceptibles dentro de su rango de transmisión.
- Para completar la infección, los smartphones susceptibles e infectados deben permanecer dentro del rango de transmisión durante todo el

tiempo de latencia.

- Un dispositivo infectado puede conectarse como máximo a un smartphone expuesto a la vez y viceversa.
- En caso de que un smartphone infectado conectado a otro se recupere como resultado del proceso de recuperación, entonces se desconectará del dispositivo expuesto, poniendo fin a todo el proceso de infección.
- Los smartphones expuestos que se conectaron a un smartphone infectado y que fue recuperado, pasarán a un estado INT debido a la cancelación del proceso de infección.
- El modelo de movimiento considera que un smartphone puede moverse una celda en cada paso de tiempo para representar que el portador del dispositivo está caminando.
- Los smartphones en estado INT volverán incondicionalmente a un estado susceptible en el siguiente paso de tiempo.
- El modelo evoluciona en pasos de tiempo $t$ iguales a 1 segundo.
- Se asume que el gusano modelado en esta investigación ataca únicamente a los dispositivos Android.

# 5

# Simulaciones y Resultados

En este capítulo, se presentan los resultados de la simulación del modelo propuesto para evaluar la dinámica de propagación de los gusanos Bluetooth en los smartphones. Para ello, se incluyen tres conjuntos de resultados. Los dos primeros analizan el efecto de factores clave en la infección de un gusano, como son: el tiempo de latencia, la posición inicial de los dispositivos infectados, el alcance de las antenas Bluetooth y las tasas de recuperación y renovación. Cada uno de estos factores se analiza para un rango de densidades de smartphones en el espacio celular (ver secciones 5.1.1 y 5.1.2). El tercer conjunto de resultados ilustra cómo la dinámica se ve afectada por las elecciones del usuario, como encender la antena, poner el dispositivo en modo descubrible o aceptar una transmisión entrante. Todas estas elecciones se realizan frente a diferentes valores de densidad de teléfonos inteligentes (véase la subsección 5.1.2). La figura 5.1 muestra un diagrama de flujo que resume los pasos de simulación del modelo introducido en este trabajo.

## 5.1. Escenario general

Para todos los casos, las simulaciones se llevan a cabo en un cuadrícula bidimensional $\mathcal{C}$ de $101 \times 101$ celdas, que representa un espacio geográfico limitado típico en una zona urbana. Cada celda representa un área de 1 $m^2$ y puede estar ocupada o no por un smartphone en el instante de tiempo $t$. Además, como ya se ha mencionado en la sección anterior, se considera una vecindad de Moore para cada celda en la posición $(i, j)$.

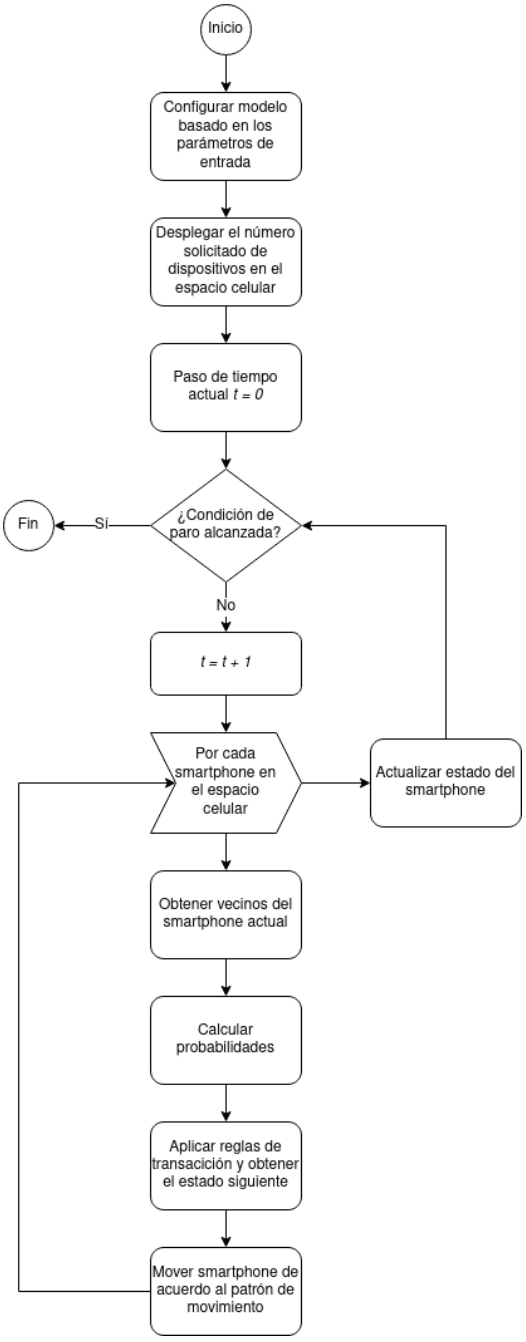



Figura 5.1: Diagrama de flujo de los pasos de la simulación del modelo propuesto

Todos los resultados de simulación presentados en la primera serie de resultados se generaron mediante simulaciones de 21,600 s (6 horas). Para cada valor de densidad de smartphones considerado, se realizaron 10 ejecuciones de simulación y se promediaron los resultados obtenidos. En todas las pruebas se consideró una población heterogénea de smartphones en la que el 84 % son dispositivos Android. También se asume que el gusano modelado en esta investigación ataca únicamente a los dispositivos Android. Además, para todos los resultados de la simulación, la densidad de smartphones $\sigma$, que se define como $\sigma = N/(101 \times 101)$ varía de 0.1 a 0.9, con incrementos de 0.1, a menos que se indique lo contrario.

Además, se consideró una tasa de infección $\beta$ con un valor de 0.9 para simular un gusano muy agresivo que permita analizar el papel que juegan los parámetros del modelo en la propagación de la infección. De igual manera, el valor correspondiente a la probabilidad de movimiento $P_{MOV}$ se mantiene en 0.1 para todos los experimentos, tratando de reproducir una velocidad de movimiento lenta dentro del espacio celular. El resto de los parámetros se describirán en cada caso de estudio. Los resultados de las simulaciones se obtienen al utilizar Netlogo 5.1.0, un entorno de modelado programable desarrollado sobre los lenguajes de programación Scala y Java para la simulación de sistemas complejos.

### 5.1.1. El impacto de los parámetros físicos en la propagación de malware

Esta subsección considera los resultados de experimentos controlados, basados en la variación de factores clave para determinar su impacto en la propagación del malware. En particular, los resultados de la simulación se obtuvieron variando el tiempo de latencia, la posición inicial de los dispositivos infectados y el alcance del Bluetooth. Para todos los resultados de simulación de esta sección, con el fin de explorar el impacto de la variación de los parámetros físicos en la propagación del malware, se asumió que los dispositivos tenían la antena encendida, estaban en modo descubrible y aceptaban todas las solicitudes de transmisión, es decir, $P_{BT} = P_D = P_{acc} = 1$.

#### 5.1.1.1. Tiempo de latencia

El tiempo que necesita el gusano para autopropagarse a otros smartphones susceptibles cercanos a través de la antena Bluetooth está relacionado

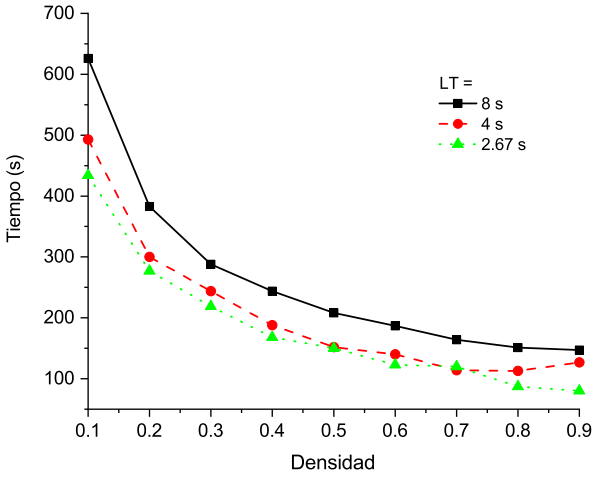
con el tiempo de latencia, que depende del tamaño del archivo del gusano y de la tasa de transferencia de datos de la antena. Así, como punto inicial de la investigación, se analizó la dinámica de propagación del malware mediante la variación de este parámetro, que afecta directamente al tiempo de latencia necesario para completar la transmisión de la carga útil del gusano a otros dispositivos, utilizando diferentes valores de densidad de smartphones. En concreto, se consideraron tasas de datos de 1 Mbps, 2 Mbps y 3 Mbps [57]. Además, según [58–62], no existe un tamaño estándar para el software malicioso; sin embargo, la tendencia es que se prefieren los tamaños pequeños debido al menor tiempo necesario para transmitirlos por la red. Por lo tanto, en esta investigación se asumió un tamaño hipotético de archivo de malware de 1 MB (1024 KB). Teniendo en cuenta este tamaño y considerando las tres velocidades de transmisión, se obtuvieron tiempos de latencia LT = 8, 4 y 2.67 s, para velocidades de transferencia de datos de 1 Mbps, 2 Mbps y 3 Mbps, respectivamente:

$$\mathrm{LT} = \frac{\text{Tamaño de archivo}}{\text{Tasa de transferencia}} \tag{5.1}$$

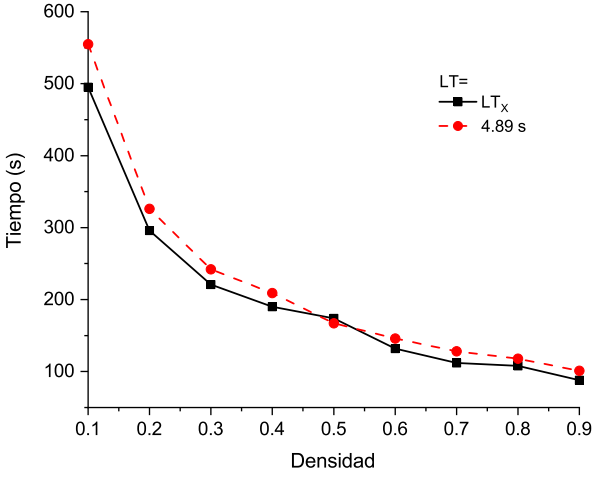
Así, se analizaron cinco escenarios diferentes. Tres de ellos resultaron de LT = 2.67, 4 y 8 s; en el cuarto se utilizó una tasa de transmisión variable, denotada como $LT_x$ de manera que, sobre la base de una distribución uniforme discreta, en cada paso de tiempo se elige uno de los tres tiempos de latencia. Por último, en el quinto escenario se consideró que el tiempo de latencia era la media de las tres tasas de transmisión, es decir, LT = 4.89 s.

Para todas las simulaciones, y dada una densidad $\sigma$, se asignó aleatoriamente la posición inicial de los smartphones en el espacio celular $\mathcal{C}$. Además, se consideró que inicialmente el 10 % de los dispositivos se encontraban en un estado infeccioso. Esta colocación aleatoria no permite que ningún otro factor interfiera en la dinámica del proceso infeccioso, como la posición inicial de los smartphones (que se presenta más adelante). Además, no se consideraron los efectos de renovación ni de renovación, es decir, $P_{IR} = 0$ y $P_{RS} = 0$, respectivamente.

La figura 5.2a muestra la variación del tiempo requerido por el gusano para infectar a todos los smartphones con sistema operativo Android (84 % de la población total) para los cuatro primeros escenarios de LT= 2.67, 4, 8, y $\mathrm{LT}_x$ s, cuando se consideran diferentes valores de densidad de $\sigma$. Como puede observarse en esta figura, cuanto mayor es el valor del tiempo de latencia, más tiempo se necesita para infectar a toda la población, como ocurre en la




(a) LT = 2.67, 4 y 8 s.




(b) LT = 4.89 s (promedio de los valores de latencia) y LT=LT$_x$ s (variando el tiempo).

Figura 5.2: Tiempo requerido para completar la propagación del gusano contra la densidad de población de smartphones, empleando $P_{MOV} = 0.1$, $P_{IR} = 0$ y $P_{RS} = 0$, $P_{BT_1} = 1$, $\beta = 0.9$ y diferentes valores para LT.

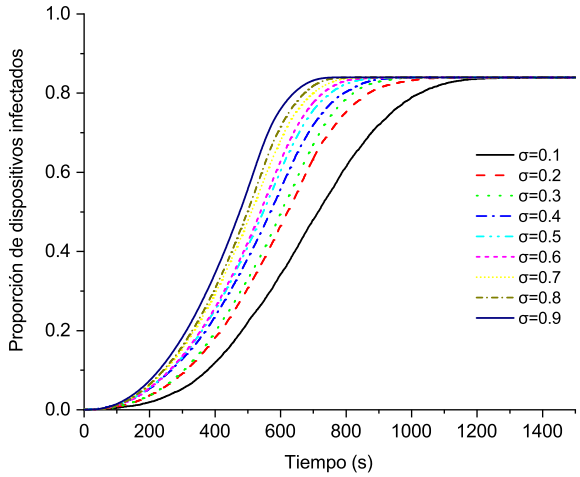
realidad. Por otro lado, hay que tener en cuenta que el tiempo necesario se reduce a medida que aumenta la densidad, ya que la probabilidad de que un usuario se mueva es menor, por lo que aumenta la probabilidad de infección al permanecer el dispositivo dentro del rango de la antena de un dispositivo infectado durante más tiempo. Por lo tanto, una mayor densidad tiene una mayor influencia que el tiempo de latencia en la propagación del gusano.

Además, la figura 5.2b compara los escenarios cuarto y quinto, demostrando que el comportamiento obtenido para LT=$LT_X$ s es muy similar al correspondiente a LT = 4.89 s, la media de los tres valores de latencia considerados. Con base en estos últimos resultados, en el resto de los experimentos de simulación se utilizará un LT = 4.89 s.

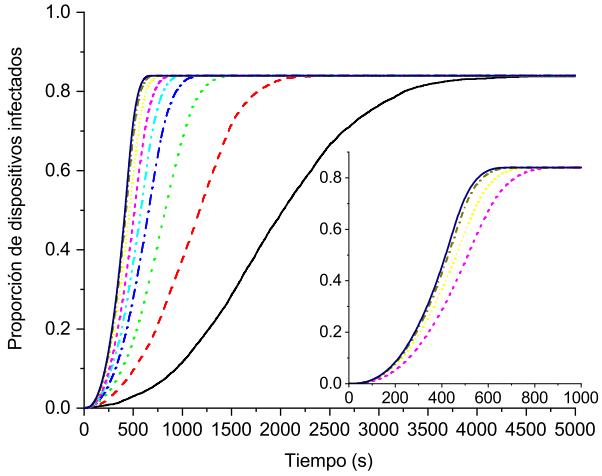
#### 5.1.1.2. Posición inicial de los dispositivos infectados

En los modelos de propagación de virus biológicos, los brotes infecciosos se simulan mediante la aparición de un único individuo infectado en el tiempo $t = 0$, a partir del cual se producirán los siguientes contagios. Así, los siguientes experimentos pretenden estudiar cómo la posición inicial del smartphone infectado influye en la evolución temporal de la propagación del gusano a otros dispositivos dentro de su rango de transmisión, con el fin de determinar las condiciones espaciales que favorecen o perjudican la dinámica de la infección. Para ello, se consideraron dos posiciones iniciales diferentes del smartphone infectado debido a la simetría del área geométrica: en una esquina y en el centro del espacio. Para ambas posiciones iniciales, se obtuvieron resultados considerando dos tipos diferentes de patrones de movimiento (ver subsección 4.1.4): Línea recta (SL) y caminata aleatoria (RW).

Las figuras 5.3a y 5.3b muestran la evolución en el tiempo de la proporción de smartphones infectados cuando la posición inicial del smartphone infectado está en el centro del espacio geográfico, para los patrones de movimiento SL y RW, respectivamente. Se puede observar que se produce una propagación más rápida del gusano para el patrón SL si la densidad es baja, $\sigma \leq 0.5$. Sin embargo, cuando la densidad es alta, $\sigma > 0.5$, la propagación del gusano evoluciona ligeramente más rápido para el patrón de movimiento RW (véase el inserto de la figura). Esto ocurre porque el patrón SL tiende a moverse a través de rutas más grandes que el RW, que se mueve localmente. Un comportamiento cualitativo similar ocurre cuando la posición inicial del smartphone infectado se sitúa en una esquina del espacio de la celda $\mathcal{C}$ y que no es mostrado por economía de espacio.




(a) Centro, Línea Recta.




(b) Centro, Caminata Aleatoria.

Figura 5.3: Proporción de los smartphones infectados con respecto al tiempo, para diferentes valores de densidad, cuando se asigna el centro del espacio geográfico como posición inicial. a) Movimiento de línea recta (SL); b) Movimiento de caminata aleatoria (RW). Todos los dispositivos tienen la antena encendida, están en modo descubrible y aceptaron todas las solicitudes de transmisión, i.e. $P_{BT} = P_D = P_{acc} = 1$

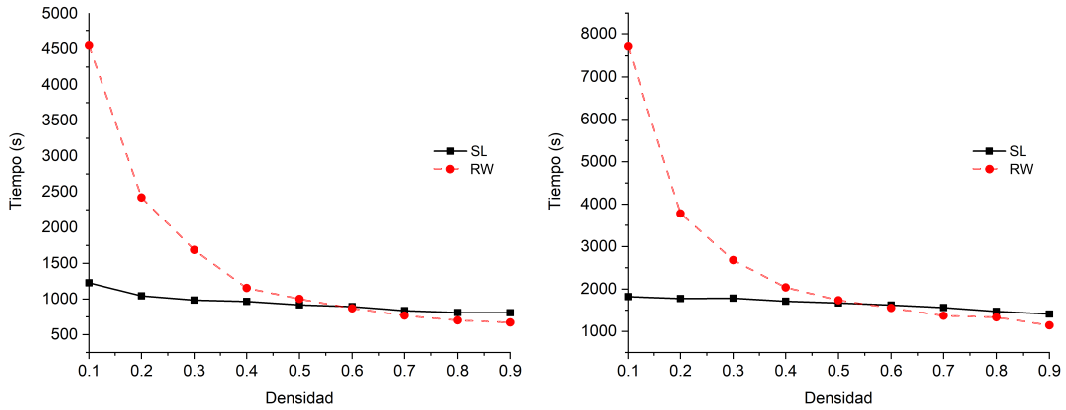
Los resultados se resumen en las figuras 5.4a y 5.4b, que corresponden al tiempo necesario para que el gusano infecte a toda la población de smartphones contra la densidad $\sigma$, para ambos patrones de movimiento SL y RW, cuando la infección comienza en el centro o en la esquina del espacio celular $\mathcal{C}$, respectivamente. Nótese que el comportamiento observado es cualitativamente similar, independientemente de la posición inicial del primer dispositivo infectado. Sin embargo, la combinación de la posición inicial del smartphone infectado y el tipo de movimiento afecta cuantitativamente al brote en términos de tiempo. En particular, el tiempo requerido cuando la infección comienza desde una esquina es aproximadamente un 40 % más largo que cuando comienza desde el centro. Esto puede observarse más claramente en la figura 5.5 que muestra el estado espacio-temporal del sistema después de 500 s para ambas posiciones iniciales. La figura 5.5a muestra el estado del sistema cuando la infección comienza en el centro, mientras que la figura 5.5b muestra el estado del sistema cuando la infección comienza en una esquina. Nótese que la posición en el centro del espacio celular favorece de forma considerable la velocidad de propagación del gusano y constituye el peor escenario para estimar el impacto de la propagación del gusano en un espacio limitado.

#### 5.1.1.3. Rango de la antena

Como se mencionó anteriormente, derivado de la falta de infraestructura de seguridad centralizada, Bluetooth tiene serias vulnerabilidades de seguridad que pueden exponer información importante de un dispositivo a otros en redes Bluetooth. Por ello, en esta subsección se analiza la propagación del gusano para antenas Bluetooth de 1 m y 10 m de alcance con el fin de evaluar el impacto. Los escenarios de simulación comenzaron utilizando sólo las antenas de 1 m de alcance y fueron aumentando el número de dispositivos con 10 m de alcance. La proporción de la población de smartphones con cada tipo de rango de antena se indicó con las variables $P_{r1}$ y $P_{r10}$, de forma que $P_{r1} + P_{r10} = 1$. El tiempo de latencia utilizado para estos experimentos fue el valor medio de 4.89 s calculado en la subsección 5.1.1.1.

Basado en los resultados de las secciones anteriores, las simulaciones se hicieron sólo cuando la infección comenzó en el centro del espacio celular $\mathcal{C}$ y con patrones de movimiento en línea recta.

Las figuras 5.6a y 5.6b muestran la evolución en el tiempo de la proporción de dispositivos infectados, para diferentes valores de la densidad de



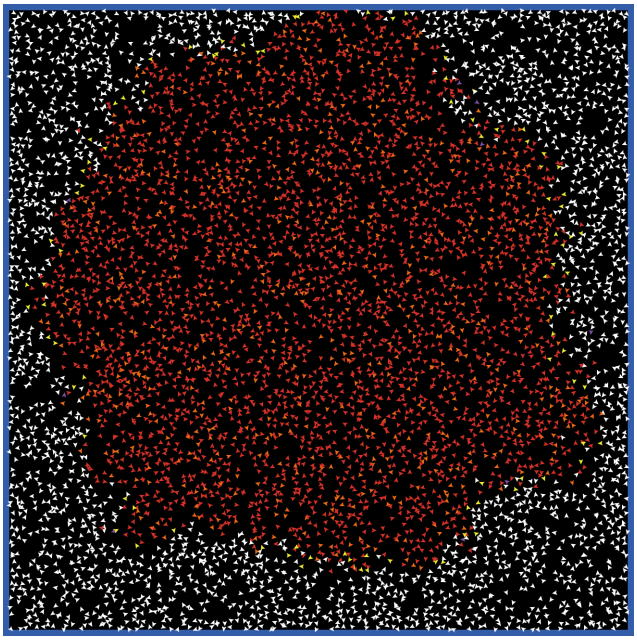

(a) Infección iniciada en el centro.

(b) Infección iniciada en la esquina.

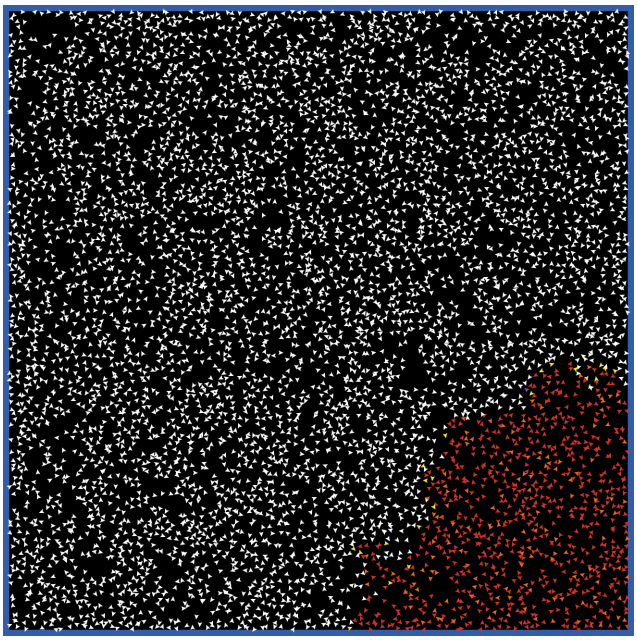
Figura 5.4: Comparación del tiempo requerido para la propagación completa del gusano contra la densidad de población de smartphones considerando múltiples patrones de movimiento.

dispositivos en el espacio celular $\mathcal{C}$, cuando se consideran dos escenarios de distribución de antenas: a) $P_{r1} = 05$ y $P_{r10} = 0.5$ y b) $P_{r1} = 0$ y $P_{r10} = 1$. Hay que destacar varios aspectos en estas figuras. En primer lugar, la velocidad de propagación del gusano es más rápida a medida que $P_{r10} \to 1$, ya que el tiempo para alcanzar la propagación completa es aproximadamente un 30 % más rápido cuando $P_{r10} = 1$; en segundo lugar, cuando la densidad $\sigma$ es mayor que 0.3, el tiempo para la propagación completa del gusano es muy similar para los dos escenarios. Esto indica claramente un valor crítico de densidad, $\sigma > 0.3$, más allá del cual no se puede evitar la propagación completa.

En la figura 5.7, el tiempo para la propagación completa del gusano se grafica contra la densidad del dispositivos para seis combinaciones diferentes de $P_{r1}$ y $P_{r10}$. Obsérvese que cuando $P_{r10} > 0.4$ y $\sigma > 0.3$, la propagación completa del gusano tarda menos de 400 s, ó 7 minutos. Sólo cuando todas las antenas tienen $r = 1$, el tiempo de propagación completa es significativamente mayor. Dado que el alcance de los nuevos dispositivos Bluetooth tiende a ser mayor, es decir, $r \geq 10$, las simulaciones demuestran el riesgo de propagación completa del gusano incluso para valores modestos de la den-



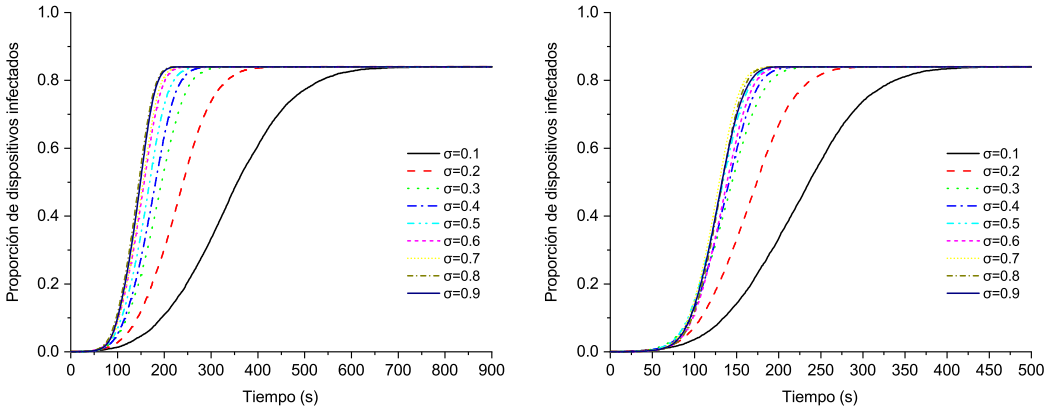
(a) Centro, $t = 500$ s.



(b) Esquina, $t = 500$ s.

Figura 5.5: Diagramas espacio-tiempo de la evolución de la infección en el tiempo 500s.

sidad de smartphones $\sigma \geq 0.3$, si la proporción de dispositivos con mayor alcance supera el 40 %.




(a) $P_{r_1} = 0.5, P_{r_{10}} = 0.5$. (b) $P_{r_1} = 0, P_{r_{10}} = 1$.

Figura 5.6: Evolución en el tiempo de infección contra la densidad de población de smartphones considerando distintos rangos de antenas Bluetooth, el dispositivo infectado inicial es ubicado en el centro del espacio celular $\mathcal{C}$ y con el patrón de movimiento SL aplicado.

### 5.1.2. Recuperación y renovación de los dispositivos

**Factor de recuperación**

Hasta ahora, todos los experimentos muestran la propagación del gusano en una red Bluetooth en la que ningún smartphone tiene un mecanismo de recuperación. Evidentemente, esta situación no refleja la realidad, ya que algunos usuarios pueden tener una copia de seguridad de la configuración personal de su smartphone o simplemente se sienten cómodos con un reinicio de fábrica. Para describir la probabilidad de que se elimine el malware si un smartphone se infecta, se realizaron y analizaron experimentos en los que la probabilidad de recuperación, $P_{IR}$, recibía valores mayores a cero. En concreto, se consideraron valores de $P_{IR} \in [0.01, 0.1]$.

Para todos los resultados de simulación presentados, se asumió que todos los dispositivos utilizaban una antena Bluetooth con un alcance de 10 m, ya que esta es la configuración más común para los dispositivos comerciales

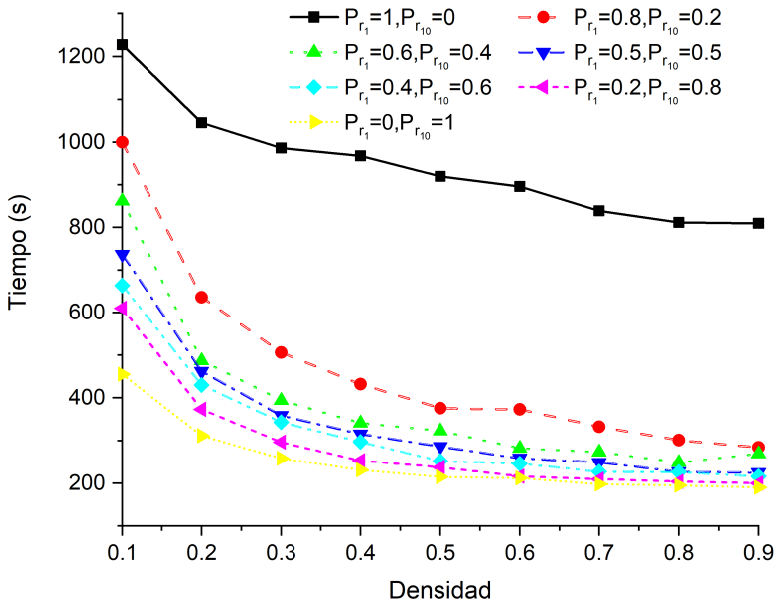



Figura 5.7: Evolución en el tiempo de la infección frente a la densidad de población de smartphones considerando diferentes rangos para las antenas Bluetooth, el dispositivo infectado se coloca primero en el centro del espacio celular C y se considera el movimiento del SL.

(smartphones, tabletas, etc.), como se describe en [57]. Además, se consideró una densidad inicial de dispositivos infectados correspondiente al 10 %.

La figura 5.8 muestra la evolución en el tiempo de la proporción de dispositivos infectados en función de la densidad de smartphones $\sigma$, para cuatro valores diferentes de la probabilidad de recuperación $P_{IR}$, cuando se utiliza el movimiento SL. Las gráficas indican que en los cuatro casos, todos los dispositivos acaban recuperándose, independientemente de la densidad $\sigma$. Sin embargo, hay diferencias interesantes entre los escenarios. Mientras que para los valores más bajos, $P_{IR} = 0.01, 0.05$, existe un pico inicial en el que la propagación supera el 10 % inicial de la población infectada que posteriormente en el tiempo evoluciona hasta eliminar el gusano de todos los dispositivos. En cambio, para valores mayores, $P_{IR} = 0.08, 0.09$, no hay un pico inicial y el gusano se elimina gradualmente. Este comportamiento indica que incluso valores modestos, $P_{IR} = 0.01$, pueden impedir la propagación del gusano.

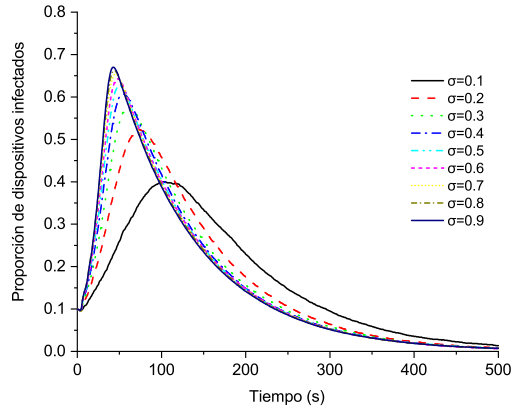
Las simulaciones mostradas en la figura 5.9 muestran el tiempo requerido para eliminar el gusano en comparación con diferentes valores de $P_{IR}$, para cuatro valores de densidad de smartphones $\sigma$ y dos patrones de movimiento, SL y RW. Esta figura indica que no hay una diferencia significativa en la recuperación de los dispositivos infectados debido al patrón de movimiento. Igualmente, existe un tiempo mínimo para eliminar el gusano de los dispositivos inicialmente infectados para cada valor de $\sigma$, tiempo que aumenta con la densidad $\sigma$ al haber más dispositivos de los que eliminar el gusano.

**Intervención del usuario**

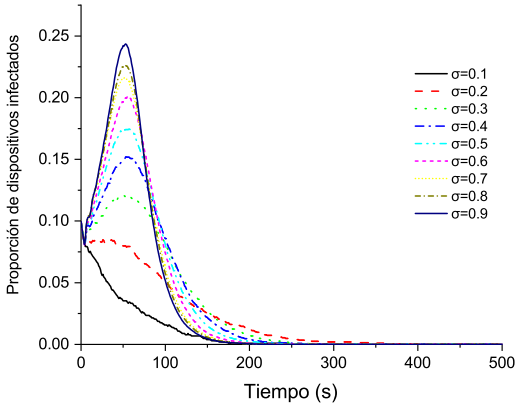
Los resultados de la simulación presentados en las secciones anteriores permitieron explorar la dinámica general de propagación del gusano en el modelo propuesto y analizar su comportamiento. Se demostró que la propagación se ve favorecida por la posición inicial del primer dispositivo infectado y el uso de antenas de largo alcance. Además, la combinación de los procesos de recuperación y renovación en la población de smartphones muestra que la infección puede llegar a ser endémica, si la densidad de dispositivos es media o grande.

En esta sección se analiza la interacción del usuario. Para ello, se consideraron tres acciones distintas: i) Activar la antena Bluetooth; ii) Poner el dispositivo en modo descubrible; y iii) Aceptar una transmisión Bluetooth entrante. Estas tres acciones se modelan con cambios en $P_{BT}$, $P_D$ y $P_{acc}$, respectivamente.

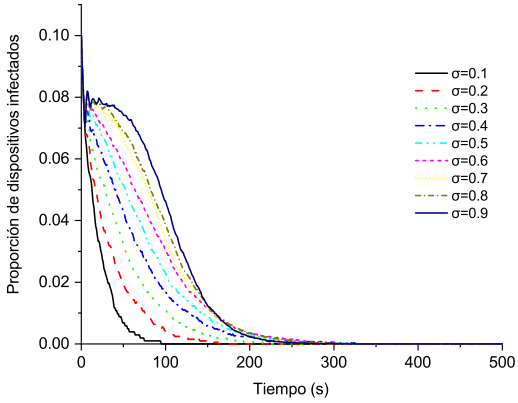
De esta forma, es posible diseñar diferentes escenarios específicos de propagación de gusanos que consideren el nivel de conciencia de ciberseguridad



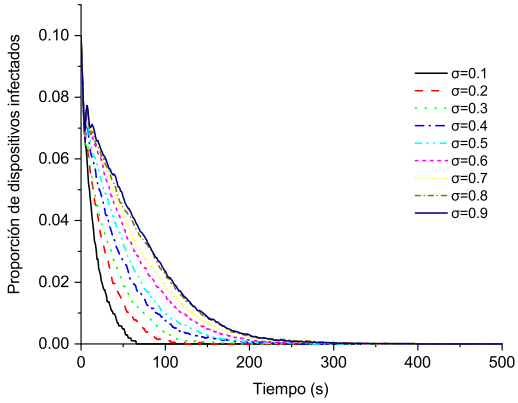

(a) $P_{IR} = 0.01$.




(b) $P_{IR} = 0.05$.

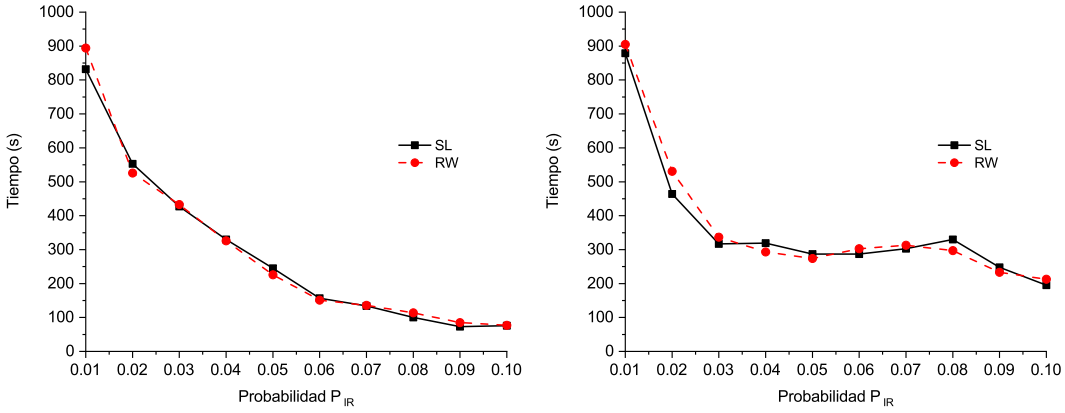



(c) $P_{IR} = 0.08$.




(d) $P_{IR} = 0.09$.

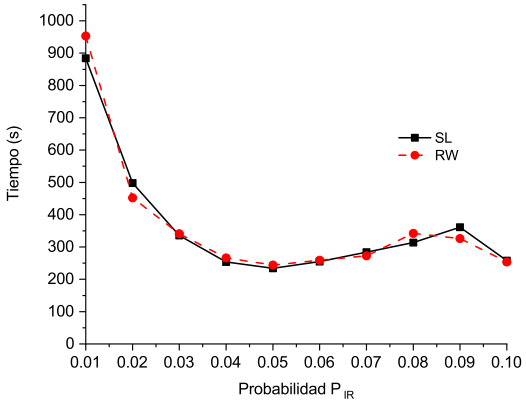
Figura 5.8: Proporción de los dispositivos infectados como función del tiempo, para diferentes valores de densidad de dispositivos $\sigma$ y variaciones en la probabilidad de recuperación $P_{IR}$



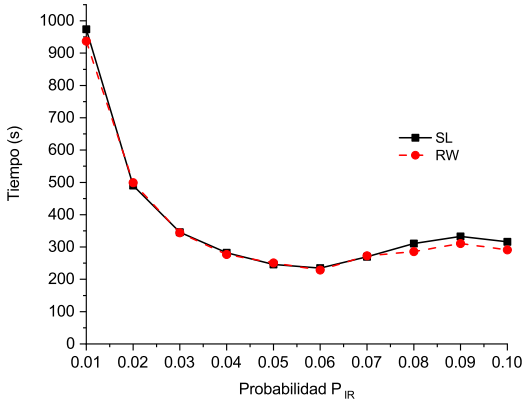

(a) $\sigma = 0.1$.




(b) $\sigma = 0.5$.




(c) $\sigma = 0.8$.




(d) $\sigma = 0.9$.

Figura 5.9: Tiempo para eliminar el gusano del 10 % inicial de dispositivos infectados contra a la probabilidad de recuperación $P_{IR}$, patrones de movimiento SL, RW y diferentes valores de densidad $\sigma$.

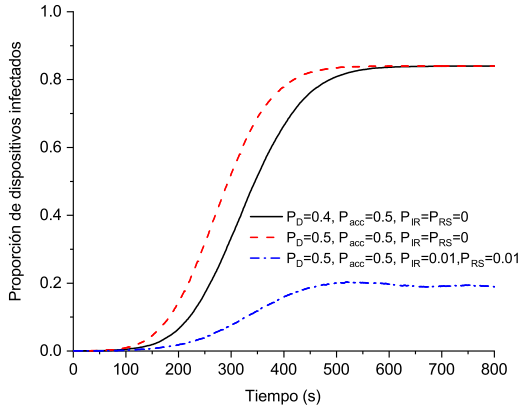
del usuario de un smartphone respecto a los riesgos inherentes al uso de estos dispositivos en redes Bluetooth. Algunos ejemplos podrían ser, un escenario en el que es posible que un usuario decida mantener la antena encendida en todo momento, $P_{BT} = 1$, pero en un modo descubrible inactivo para poder conectarse sólo con otros dispositivos previamente emparejados, $P_D = 0$; o cuando un usuario mantiene la antena encendida, $P_{BT} = 1$, y activa el modo descubrible, $P_D = 1$, pero el usuario sólo acepta algunas transferencias, $0 < P_{acc} < 1$. Por otra parte, además de los patrones de movimiento SL y RW considerados en las simulaciones anteriores, esta sección también presenta los resultados de la simulación para el movimiento mixto con pausas (MMwP), definido en la sección 4.1.4. El objetivo es analizar el comportamiento de la propagación del malware cuando se tiene en cuenta un movimiento humano más realista. Este patrón de movimiento considera tiempos de pausa aleatorios después de que un agente alcance un punto de destino antes de moverse a uno nuevo (véase la sección 4.1.4). Esta modificación hace que el MMwP sea más realista que los movimientos SL y RW. Dado que el modelo considera el comportamiento humano casual, supone que los usuarios suelen hacer una pausa durante algún tiempo después de alcanzar un destino en particular.

Para todas las simulaciones, se colocó un smartphone infectado en el centro del espacio geográfico y $P_{r10} = 1$. Se consideraron dos valores de densidad de smartphones en el espacio celular, alta (0.9) y baja (0.3).

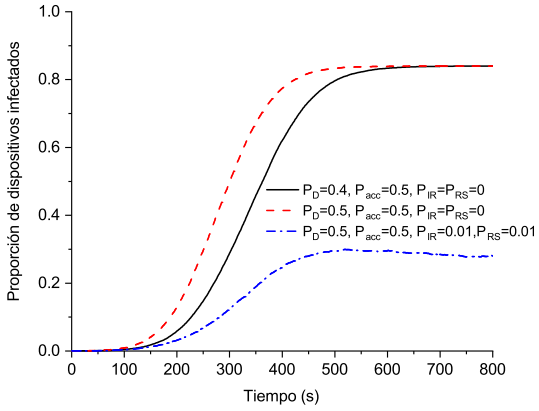
Las figuras 5.10 y 5.11 muestran los resultados de la simulación para varias combinaciones de valores de $P_{IR}$, $P_{RS}$, $P_D$ y $P_{acc}$. Los dos últimos valores de probabilidad representan el nivel de conciencia de ciberseguridad del usuario. Las figuras 5.10a-5.10c corresponden a una densidad baja, $\sigma = 0.3$, mientras que las figuras 5.11a-5.11c corresponden a una densidad alta, $\sigma = 0.9$. En ambos casos se analizan los tres patrones de movimiento SL, RW y MMwP. Como puede observarse en las figuras 5.10 y 5.11, los resultados de la simulación indican que incluso cuando no se incluyen las probabilidades de recuperación y renovación, una mejor conciencia de ciberseguridad del usuario da lugar a una propagación más lenta del malware, independientemente de la densidad del smartphone. Además, los resultados también indican que la conciencia de ciberseguridad, representada por el hecho de que la antena tenga activado el modo descubrible y la aceptación de las conexiones entrantes, desempeña un papel decisivo en la expansión del gusano. Esto ocurrió aunque la antena Bluetooth estuviera permanentemente activada ($P_{BT} = 1$) durante todas las simulaciones e incluso sin un mecanismo de recuperación. Además, los resultados de las figuras 5.10 y 5.11 también indican que cuando

se tienen en cuenta los procesos de recuperación y renovación, el gusano ya no es capaz de afectar a toda la población de dispositivos y su capacidad de propagación se reduce, aunque sin eliminarlo por completo del espacio celular $C$.

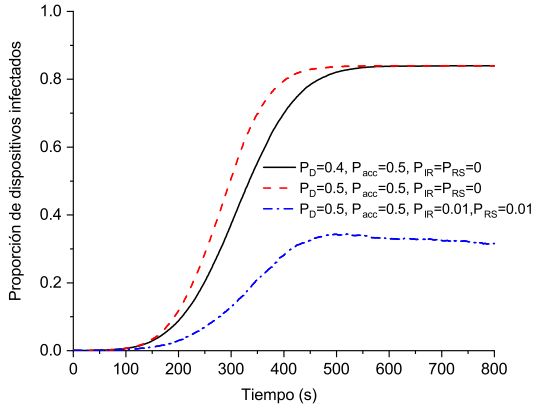
Para analizar los efectos de los diferentes patrones de movimiento en la propagación del malware, la figura 5.12a muestra la proporción de dispositivos infectados a lo largo del tiempo para los patrones de movimiento SL, RW y MMwP, para $P_D = P_{acc} = 0.5$, $P_{IR} = P_{RS} = 0.01$ y $\sigma = 0.3$ (baja densidad), mientras que la figura 5.12b utiliza los mismos valores de parámetros para $\sigma = 0.9$ (alta densidad). En ambos casos, se observa que la mayor proporción de dispositivos infectados se produce con el movimiento MMwP. Esto es consecuencia de las pausas en el patrón de movimiento que reducen las interrupciones de la transmisión y favorecen la infección del malware y la posibilidad de moverse en todas las direcciones, incluso en entornos de baja densidad. Para SL y RW, la propagación del malware cambia en función de la densidad. Para entornos de baja densidad, se consigue una mayor proporción de infección con el movimiento RW; esto se debe a que los usuarios tienden a moverse en la misma ubicación y, teniendo en cuenta que hay muchos espacios disponibles a los que moverse, se favorece la propagación del malware. Para entornos de alta densidad, se consigue una mayor población de dispositivos infectados con el movimiento SL, porque los usuarios de smartphones tienden a moverse por rutas más amplias que con el patrón RW, lo que no se ve favorecido por los reducidos espacios existentes entre dispositivos. Estos resultados confirman la importancia de utilizar patrones de movimiento realistas para reproducir más fielmente el comportamiento de propagación del malware en el espacio celular $\mathcal{C}$.




(a) Línea Recta, $\sigma = 0.3$.

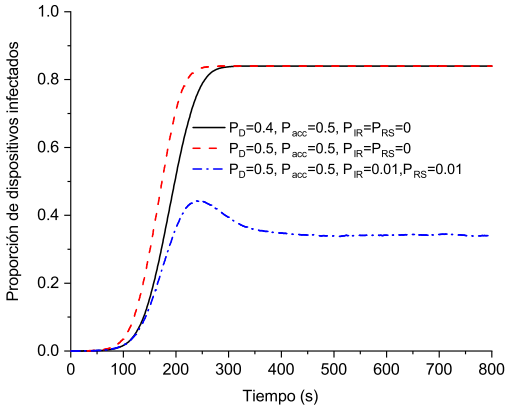



(b) Caminata Aleatoria, $\sigma = 0.3$.

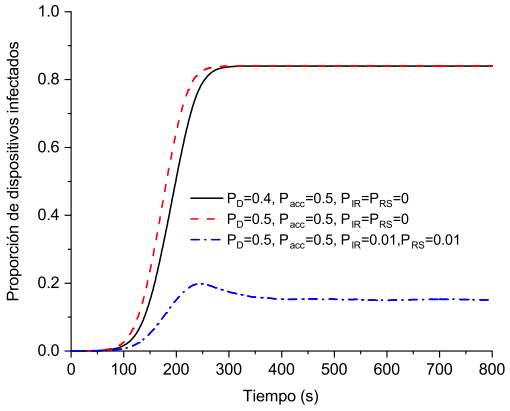



(c) Movimiento Mixto con Pausas, $\sigma = 0.3$.

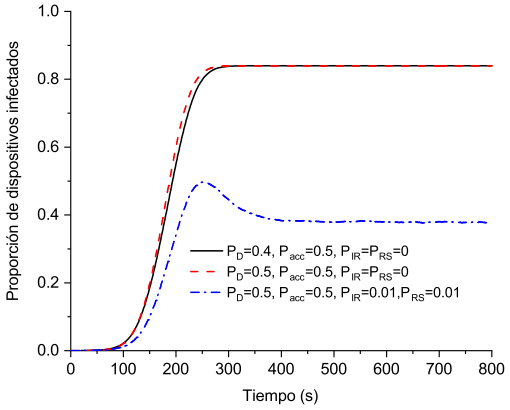
Figura 5.10: Efecto de las probabilidades de recuperación ($P_{IR}$) y renovación $P_{RS}$) en la evolución en el tiempo para diferentes valores de $P_{BT}$ y $P_D$, distintos patrones de movimiento considerando el inicio del brote en el centro del espacio celular, y una densidad de población $\sigma = 0.3$.




(a) Línea Recta, $\sigma = 0.9$.

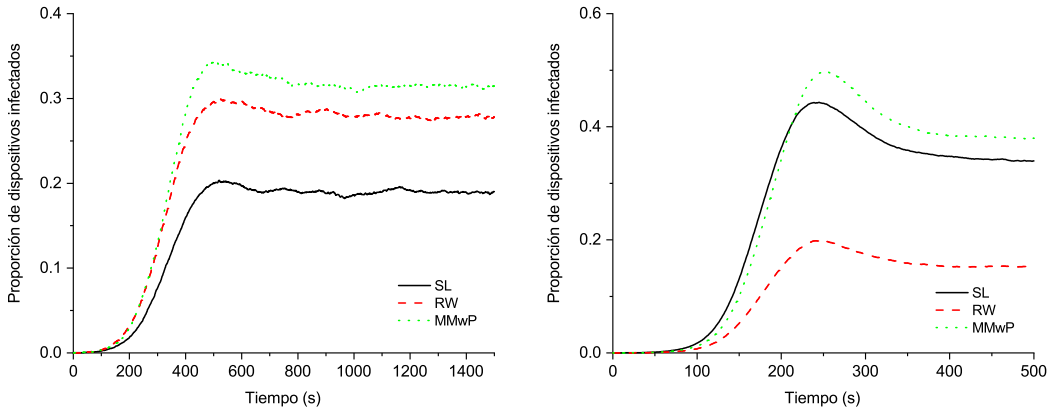



(b) Caminata aleatoria, $\sigma = 0.9$.




(c) Movimiento Mixto con Pausas, $\sigma = 0.9$.

Figura 5.11: Efecto de las probabilidades de recuperación ($P_{IR}$) y renovación $P_{RS}$) en la evolución en el tiempo para diferentes valores de $P_{BT}$ y $P_D$, distintos patrones de movimiento considerando el inicio del brote en el centro del espacio celular, y una densidad de población $\sigma = 0.9$




(a) $\sigma = 0.3$. (b) $\sigma = 0.9$.

Figura 5.12: Evolución en el tiempo de los dispositivos infectados con distintos patrones de movimiento para $P_D = P_{acc} = 0.5, P_{IR} = P_{RS} = 0.01$. El comienzo de la epidemia es en el centro del espacio celular y con una densidad de población $\sigma = 0.3$ y $\sigma = 0.9$

# 6

# Conclusiones y Trabajo Futuro

## 6.1. Validación de la hipótesis

De acuerdo con los resultados obtenidos en el capítulo 5, se puede afirmar que .Es posible simular de forma fiel y simple la propagación de malware tipo gusano cuyo vector de infección depende de la proximidad física con otros dispositivos, mediante el uso del paradigma de AC, agentes y ciencia de redes". El uso de agentes para representar a los smartphones permite contar con una abstracción flexible que permite incluir, modificar o eliminar atributos que pertenecen a los dispositivos de forma simple. La interacción entre los dispositivos fue modelada de forma consistente al emplear funciones de transición del AC.

## 6.2. Conclusiones

Inspirado en los modelos epidemiológicos compartimentados, este trabajo de tesis presentó un nuevo modelo espacio-temporal explícito para caracterizar la dinámica de propagación del malware tipo gusano en los smartphones mediante un autómata celular bidimensional. Este modelo tiene en cuenta las características individuales de cada dispositivo, como la configuración de seguridad, el tiempo de latencia para transmitir el gusano y el tipo de sistema operativo, entre otras. En las simulaciones realizadas se implementaron diferentes patrones de movimiento que permitieron estudiar cómo la demografía del usuario afectaba a la mecánica de propagación del gusano. El trabajo

analizó diferentes escenarios de simulación en los que también se tuvo en cuenta la conciencia de los usuarios sobre los riesgos inherentes al uso de dispositivos inteligentes en redes Bluetooth. Para ello, se obtuvieron diversos valores de probabilidad que describen la aceptación de la comunicación entrante y los efectos de la recuperación e inmunidad a las amenazas al disponer de algún mecanismo de restauración o al aplicar una copia de seguridad. Además, como la heterogeneidad de los dispositivos inteligentes va más allá del tipo de sistema operativo, también se consideraron los diferentes tipos de antenas integradas en los dispositivos inteligentes según las especificaciones del estándar Bluetooth, cuya tasa de transmisión y alcance afectan directamente a la velocidad de propagación. Basándose en todos estos aspectos, se llevó a cabo un análisis de la dinámica de propagación para determinar cómo podría propagarse un gusano de Bluetooth en determinados escenarios. Los resultados de la simulación indican que el alcance y la velocidad de la antena Bluetooth son factores cruciales a tener en cuenta, ya que dan al atacante más posibilidades de llegar a un mayor número de dispositivos. Además, la combinación de la posición inicial del smartphone infectado y el tipo de movimiento también afectaron al brote de la epidemia en términos de tiempo. En particular, se observó que la posición en el centro del espacio geográfico favorece en gran medida la propagación del gusano cuando se consideran espacios limitados. Esto podría ser importante cuando un atacante propaga virus o comete otros ciberdelitos en zonas limitadas y concurridas. Además, los resultados de la simulación indicaron que la densidad de dispositivos también tiene un impacto en la propagación del gusano. Cuando la densidad es baja, la velocidad de propagación es lenta; a medida que la densidad aumenta, el gusano se propaga mucho más rápido, ya que los dispositivos están lo suficientemente cerca unos de otros para facilitar el contacto y la propagación del gusano. Por otra parte, los resultados de la simulación de dos patrones de movimiento diferentes, caminata aleatoria y la línea recta; indican que el patrón de línea recta favorece la propagación del gusano en espacios geográficos con baja densidad de smartphones. Finalmente, cuando se simuló un patrón de movimiento más realista, denominado Movimiento Mixto con Pausas, el número de dispositivos infectados aumentó. Además, cuando no se tienen en cuenta los mecanismos de protección, los resultados indican que el número máximo de smartphones infectados se alcanza en un tiempo reducido, como se esperaba. Todos estos resultados indican, por un lado, que las zonas concurridas que implican una alta densidad de dispositivos, pueden ser ideales para la propagación de malware tipo gusano en

dispositivos Bluetooth y, por otro, que la intervención del usuario es de importancia clave para limitar el efecto de la propagación de los gusanos. En futuras investigaciones, el modelo podría analizar los efectos de patrones de movimiento humano más realistas, como el origen-destino, y zonas geográficas más detalladas, modelos de comunidad o una combinación de ambos. El modelo podría ampliarse más allá de Bluetooth para incluir otros medios de transmisión.

# Bibliografía


[1] J. F. Kurose and K. W. Ross, *Computer Networking A Top-Down Approach*. Pearson, 2012.

[2] Statista, "Number of smartphone subscriptions worldwide from 2016 to 2021, with forecasts from 2022 to 2027." Accessed: 2022-10-13.

[3] H. Xiang, *Bluetooth-base Worm Modeling And Simulation*. PhD thesis, University of Central Florida, jan 2007.

[4] R. Nuwer, "Why is Bluetooth Called Bluetooth? (Hint: Vikings!) — Smart News — Smithsonian," 2012. Accessed: 2020-15-20.

[5] S.-M. Cheng, W. C. Ao, P.-Y. Chen, and K.-C. Chen, "On Modeling Malware Propagation in Generalized Social Networks," *IEEE Communications Letters*, vol. 15, pp. 25–27, jan 2011.

[6] J. T. Jackson and S. Creese, "Virus Propagation in Heterogeneous Bluetooth Networks with Human Behaviors," *IEEE Transactions on Dependable and Secure Computing*, vol. 9, pp. 930–943, nov 2012.

[7] J. W. Mickens and B. D. Noble, "Modeling epidemic spreading in mobile environments," in *Proceedings of the 4th ACM workshop on Wireless security - WiSe '05*, (New York, New York, USA), p. 77, ACM Press, 2005.

[8] A.úster Sabater@, A. M. Martín del Rey, and G.íguez Sánchez@, "Simulación de la propagación del malware: Modelos continuos vs. modelos discretos," *RECSI XIII: Actas de la XIII Reunión Española sobre Criptología y Seguridad de la Información. Alicante, 2-5 de septiembre de 2014, 2014, ISBN 978-84-9717-232-0, págs. 139-144*, pp. 139–144, 2014.

[9] Á. M. del Rey and G. R. Sánchez, "A CA Model for Mobile Malware Spreading Based on Bluetooth Connections," in *International Joint Conference SOCO'13-CISIS'13-ICEUTE'13. Advances in Intelligent Systems and Computing*, pp. 619–629, Springer, Cham, 2014.

[10] M. Frodigh, P. Johansson, and P. Larsson, "Wireless ad hoc networking - the art of networking without a network," *Ericsson Review (English Edition)*, vol. 77, no. 4, pp. 248–263, 2000.

[11] S. Glisic, *Advanced Wireless Networks Cognitive , Cooperative and Opportunistic 4G Technology*. Wiley, 2006.

[12] G.ález@, M. E. Lárraga, and L. Alvarez-Icaza, "Worm Propagation Modeling Considering Smartphones Heterogeneity and People Mobility," in *Proceedings of the 2017 International Conference on Applied Mathematics, Modeling and Simulation (AMMS 2017)*, vol. 153, (Shanghai, China), pp. 147–152, Atlantis Press, nov 2017.

[13] Bluetooh SIG, "Our History — Bluetooth Technology Website." Accessed: 2020-09-20.

[14] IEEE Society, *Wireless medium access control (MAC)and physical layer (PHY) specifications forwireless personal area networks (WPANs)*. Pearson, 2005.

[15] Ericsson Technology Licensing, "Scatternet - Part 1: Baseband vs. Host Stack Implementation," 2004.

[16] F. B. Cohen, *A Short Course on Computer Viruses*. Wiley, 2 edition ed., 1994.

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

[18] V. Bontchev, "Current Status of the CARO Malware Naming Scheme," 2005. Accessed: 2020-09-21.

[19] BitDefender, "Malware History," 2010. Accessed: 2020-09-20.

[20] Computer Economics, "Annual Worldwide Economic Damages from Malware Exceed $13 Billion — Computer Economics – for IT metrics, ratios, benchmarks, and research advisories for IT management," 2007. Accessed: 2020-09-21.

[21] Center for Strategic and International Studies, "Net Losses: Estimating the Global Cost of Cybercrime — Center for Strategic and International Studies," 2014. Accessed: 2020-09-21.

[22] Guanhua Yan and S. Eidenbenz, "Modeling Propagation Dynamics of Bluetooth Worms (Extended Version)," *IEEE Transactions on Mobile Computing*, vol. 8, pp. 353–368, mar 2009.

[23] F-Secure Labs, "Bluetooth-Worm:SymbOS/Cabir Description — F-Secure Labs." Accessed: 2020-09-20.

[24] F-Secure Labs, "Bluetooth-Worm:SymbOS/Commwarrior.B Description — F-Secure Labs." Accessed: 2020-09-20.

[25] Kaspersky, "Mobile Malware Evolution: An Overview, Part 1," 2006.

[26] Kaspersky, "Five stories about Cabir, the first malware for smartphones," 2014.

[27] N. Husted and S. Myers, "Why mobile-to-mobile wireless malware won't cause a storm," *LEET 2011 - 4th USENIX Workshop on Large-Scale Exploits and Emergent Threats: Botnets, spyware, Worms, and More*, 2011.

[28] Bluetooth SIG, "Bluetooth market update 2018," tech. rep., Bluetooth SIG, 2018. Accessed: 2020-09-22.

[29] Armis Labs, "BlueBorne Information from the Research Team - Armis Labs," 2017. Accessed: 2020-09-20.

[30] B. Seri and G. Vishnepolsky, "The dangers of Bluetooth implementations: Unveiling zero day vulnerabilities and security flaws in modern Bluetooth stacks," *ArmisLabs*, pp. 1–38, 2017.

[31] A. M. Lonzetta, P. Cope, J. Campbell, B. J. Mohd, and T. Hayajneh, "Security vulnerabilities in bluetooth technology as used in iot," *Journal of Sensor and Actuator Networks*, vol. 7, no. 3, p. 28, 2018.

[32] P.Ñeill@, "India is forcing people to use its covid app, unlike any other democracy," 2020.

[33] A. Illmer, "Singapore reveals Covid privacy data available to police," 2021.

[34] P.Ñeill@, T. Ryan-Mosley, and B. Johnson, "A flood of coronavirus apps are tracking us. Now it's time to keep track of them.," 2020.

[35] European Commission, "How tracing and warning apps can help during the pandemic — European Commission," 2020.

[36] BBVA, "How do COVID-19 tracing apps work and what kind of data do they use?," 2020.

[37] Health Canada, "Download COVID Alert: Canada's exposure notification app - Canada.ca," 2020.

[38] New Zealand Government, "NZ COVID Tracer app — Unite against COVID-19," 2020.

[39] R. Pegoraro, "Google and Apple-supported coronavirus tracking apps land from states," 2020.

[40] X. Xiao, P. Fu, C. Dou, Q. Li, G. Hu, and S. Xia, "Design and analysis of seiqr worm propagation model in mobile internet," *Communications in nonlinear science and numerical simulation*, vol. 43, pp. 341–350, 2017.

[41] J. Von Neumann and A. W. Burks, *Theory of Self-Reproducing Automata*, vol. 18. University of Illinois Press, oct 1966.

[42] G. J. Martínez, A. Adamatzky, and H. V. McIntosh, "Localization Dynamics in a Binary Two-Dimensional Cellular Automaton: The Diffusion Rule," in *Game of Life Cellular Automata*, pp. 291–315, London: Springer London, 2010.

[43] H. W. Hethcote, "Three Basic Epidemiological Models," pp. 119–144, Springer, Berlin, Heidelberg, 1989.

[44] W. O. Kermack and A. G. McKendrick, "A Contribution to the Mathematical Theory of Epidemics," *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences*, vol. 115, pp. 700–721, aug 1927.

[45] W. O. Kermack and A. G. McKendrick, "Contributions to the Mathematical Theory of Epidemics. II. The Problem of Endemicity," *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences*, vol. 138, pp. 55–83, oct 1932.

[46] W. O. Kermack and A. G. McKendrick, "Contributions to the Mathematical Theory of Epidemics. III. Further Studies of the Problem of Endemicity," *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences*, vol. 141, pp. 94–122, jul 1933.

[47] S. Peng, S. Yu, and A. Yang, "Smartphone Malware and Its Propagation Modeling: A Survey," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 2, pp. 925–941, 2014.

[48] S. Peng, G. Wang, and S. Yu, "Modeling the dynamics of worm propagation using two-dimensional cellular automata in smartphones," *Journal of Computer and System Sciences*, vol. 79, pp. 586–595, aug 2013.

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

[50] Y. Hu, "Cellular Automata Model to Simulate the Spreading of Mobile Phone Messages Virus," *Journal of Information and Computational Science*, vol. 10, no. 11, pp. 3579–3586, 2013.

[51] Y. Song and G.-P. Jiang, "Modeling malware propagation in wireless sensor networks using cellular automata," in *IEEE Int. Conference Neural Networks & Signal Processing*, (Zhenjiang, China), pp. 623–627, 2008.

[52] S. Peng and G. Wang, "Worm propagation modeling using 2D cellular automata in bluetooth networks," *Proc. 10th IEEE Int. Conf. on Trust, Security and Privacy in Computing and Communications, TrustCom 2011, 8th IEEE Int. Conf. on Embedded Software and Systems, ICESS 2011, 6th Int. Conf. on FCST 2011*, pp. 282–287, 2011.

[53] Á. M. del Rey and G. R. Sánchez, "A ca model for mobile malware spreading based on bluetooth connections," in *International Joint Conference SOCO'13-CISIS'13-ICEUTE'13* (Á. Herrero, B. Baruque, F. Klett, A. Abraham, V. Snášel, A. C. de Carvalho, P. G. Bringas, I. Zelinka, H. Quintián, and E. Corchado, eds.), pp. 619–629, Springer, Springer International Publishing, 2014.

[54] A. M. del Rey, A. H. Encinas, J. M. Vaquero, A. Q. Dios, and G. R. Sánchez, "A cellular automata model for mobile worm propagation," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 9108, pp. 107–116, Springer, Cham, 2015.

[55] S. Wolfram, *Cellular Automata and Complexity*, vol. 1. Addison-Wesley Pub. Co, 2002.

[56] G.ález-García@, M. E. Lárraga, and L. Alvarez-Icaza, "Modeling the Spatio-Temporal Dynamics of Worm Propagation in Smartphones Based on Cellular Automata," in *Proceedings - UKSim-AMSS 2016: 10th European Modelling Symposium on Computer Modelling and Simulation*, pp. 196–201, 2017.

[57] J. Padgette, J. Bahr, M. Batra, M. Holtmann, R. Smithbey, L. Chen, and K. Scarfone, "NIST Special Publication 800-121 Revision 2 Guide to Bluetooth Security," tech. rep., National Institute of Standars and Technology, 2017.

[58] G. Yan and S. Eidenbenz, "Bluetooth worms: Models, dynamics, and defense implications," *Proceedings - Annual Computer Security Applications Conference, ACSAC*, pp. 245–256, dec 2006.

[59] U. Khan, "12 million people suffered a computer virus attack in the last six months - Telegraph," 2009. Accessed:2020-09-25.

[60] H. Pilz and M. Morgenstern, "Useful and useless statistics about viruses and anti-virus programs," 2010.

[61] R. Poston, "How large is a piece of Malware? – Naked Security," 2010. Accessed: 2020-09-21.

[62] T. Marques, "PNG Embedded – Malicious payload hidden in a PNG file," 2016. Accessed: 2020-09-22.