Bluetooth Worm Propagation in Smartphones: Modeling and Analyzing Spatio-Temporal Dynamics

GABRIEL GONZÁLEZ[1], **MARÍA ELENA LÁRRAGA**[1], **LUIS ALVAREZ-ICAZA**[1], **(Member, IEEE), AND JAVIER GOMEZ**[2]

[1]Instituto de Ingeniería, Universidad Nacional Autónoma de México, Coyoacán 04510, Mexico
[2]Facultad de Ingeniería, Universidad Nacional Autónoma de México, Coyoacán 04510, Mexico

Corresponding authors: María Elena Lárraga (mlarragar@iingen.unam.mx) and Gabriel González (ggonzalezga@iingen.unam.mx)

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.

INDEX TERMS Bluetooth devices, cellular automata, discrete-time systems, epidemic model, malware propagation, smartphones, systems modeling, spatiotemporal phenomena.

I. INTRODUCTION

Mobile telephony use is growing rapidly around the world. According to Statista [1], the number of mobile phone users was forecasted to reach 2.87 billion by 2020. Smart device security heads the list of concerns of all companies, as almost all their employees routinely access corporate data through them. For this reason, keeping confidential information out of reach of unauthorized people is top priority.

The associate editor coordinating the review of this manuscript and approving it for publication was Amjad Gawanmeh.

IBM Security and the Ponemon Institute have estimated that in 2018 the average global cost of a data breach was $3.86 million, a 6.4% increase from the 2017 report, which also showed that 47% of the attacks come from cyber-crime [2]. Because of the Internet's intensive use, a data breach is no longer a problem that only affects large companies. Exposure to potential risks and threats now includes end users using smartphones, tablets, laptops, and workstations. These devices store sensitive information, such as social network accounts, bank account data, credit card numbers, and personal information, a highly attractive target for malware developers.

The term malware comes from the contraction of malicious software. It usually defines a wide range of hostile and intrusive operating system software applications designed to access user information. Since many computer systems lack a good security design or allow simple user access, the term malware covers only those programs written with the specific purpose of interrupting a system's normal operation. For this reason, applications with security flaws are not considered malware since their defects and poor design were not deliberately implemented [3]. Currently, the development and spreading of malware to steal personal information is a business worth billions of dollars a year.

There is a wide range of malware types and multiple spreading channels. This paper focuses on worm-type malware, which can propagate through Bluetooth antennas by making copies of itself and sending them to other devices in its proximity without any action or knowledge of the infected smartphone owner.

Bluetooth is a brand name defined by the Bluetooth Special Interest Group in 1994 [4], [5] and standardized as IEEE 802.15.1 [6]. This standard of wireless short-range transmission has been implemented through several devices such as smartphones, headsets, laptops, hands-free for cars, etc. It might have seemed that the old days of Cabir in 2004 [7] and CommWarrior in 2005 [8] of malware that spread through Bluetooth antennas were over. While Cabir's propagation method via Bluetooth was quite original and harmless [9], [10], it was short-lived and depended heavily on the proximity of the target device. Besides, in 2004, less than 2% of the market was occupied by Bluetooth devices, making a mobile malware outbreak in the short or medium-term unlikely [11]. Finally, Wi-Fi provided an even superior propagation mechanism for mobile-to-mobile malware since it did not require authentication, inasmuch as its traffic was easier to trace and falsify compared to Bluetooth. Similarly, Wi-Fi is always on, unlike Bluetooth, which must be turned on, and in general, a discoverable mode to be exploited by malware. Another important reason why Bluetooth antennas were not considered as an attack vector was that the first versions of the standard had many errors, communication problems, and latency issues, which caused Bluetooth to fall into disuse for many years. During all these years, attackers ignored Bluetooth and wrote malware through other vectors, such as MMS, SMS, and Wi-Fi, mainly.

Many of the limiting factors that persuaded attackers not to consider Bluetooth have changed in recent years. Bluetooth has solved many of the reliability and performance issues it used to experience. At the same time, the number of Bluetooth devices has skyrocketed, and the number of apps and devices now using Bluetooth is unprecedented (according to Bluetooth 2018 market update, this year, the number of devices enabled with this technology reached 4 billion [12]). While other attack vectors such as WiFi and currently 4G-5G networks remain faster ways to attack mobile devices, Bluetooth, by its sheer number of apps and devices, is no longer a technology that could be considered risk-free. Since Bluetooth lacks a centralized security infrastructure and the risks are increasing as this technology becomes more widespread around the world. As a result, in the last years, serious security vulnerabilities have occurred. One of them is BlueBorne, a recently published attack vector that exploits security gaps in Bluetooth classic connections and can be used to execute malicious codes on affected devices [13], [14]. BlueBorne requires no user interaction and only needs the Bluetooth antenna to be on. More recently, in 2020, BlueFrag security vulnerability allowed code execution over Bluetooth in some Android devices [15]. In BlueFrag, a remote attacker could silently execute an arbitrary code with the Bluetooth daemon's privileges without requiring any user interaction. In order for BlueFrag to work, it is necessary to know the target device's Bluetooth MAC address, which in most cases can be deduced from the Wi-Fi MAC address. On the other hand, from 2016 onwards, when Bluetooth version 5 was launched, Bluetooth was able to increase transmission capacity eight times and the range up to 200 m (outdoors) or 40 m (indoors). This version widely encouraged the use of Bluetooth technology, especially for the IoT. Recently, derived from COVID-19, many governments and companies are thinking of ways to contain the pandemic using Bluetooth through so-called corona tracking apps. These apps are already widely used in some countries, such as India, Singapore, and Australia [16]–[23]. COVID-19 apps require that Bluetooth always be on, which is attractive to malware developers. New malware may therefore spread via Bluetooth in the upcoming years. Analyzing and understanding the spread of malware is thus of great importance. Undoubtedly, efficient methods to detect malware types are essential to fight Bluetooth malware. Besides, mathematical and computational modeling are powerful tools for understanding malware propagation and exploring the impact of various parameters on different scenarios. However, these models must reflect reality in the best way possible. Although models cannot answer all questions, we believe that more updated malware propagation models for Bluetooth will provide answers that can help to solve the puzzle about better understanding and reevaluating the likelihood of malware infection, even in crowded environments [24].

Since Bluetooth worms attack and infect devices in their proximity, malware propagation shows a strong similarity with the self-replicating behavior and propagation of biological viruses. Consequently, a common approach to modeling this behavior is to use classical propagation theories from epidemiology [25]. Most mathematical models for predicting mobile malware spreading by Bluetooth are based on continuous modeling, such as systems of ordinary differential equations [26]–[33]. Although these models are very useful in describing global behavior and are able to consider some factors known to affect virus propagation, such as human behavior, device heterogeneity, and measures to prevent infections, they are not able to simulate the local dynamic interactions between all devices in a given space.

As in the case of infectious biological diseases, modeling the interactions between individuals reflects a more detailed behavior that better resembles real-life scenarios. In this regard, models based on cellular automata (CA) have become a well-established alternative for simulating, analyzing, and understanding worm behavior and propagation [34]–[40]. CA are discrete-time dynamic systems of interacting individuals in a cell space [41], the state of which is also discrete. The state of each one of the individuals is updated in parallel at each discrete timestep, following a simple homogeneous set of rules. When this set of rules induces stochastic processes, CA can be considered a paradigm for a large dynamic system in which many particles are allowed to interact under certain local neighborhood rules. In this way, new individual states are chosen according to some probability distributions. Therefore, the behavior of the complete system depends on the nature of the interaction between individuals. Thus, CA can be seen as locally interacting Markov chains where it is theoretically possible to join all the individuals in the cell space and propose a very high dimension dynamic system, the structure of which changes dramatically with time in a nonlinear fashion in order to represent all feasible interactions between individuals.

Peng *et al.* [34], [38] proposed a CA model to simulate the dynamics of worm propagation in Bluetooth networks based on the consideration of the spread degree of infected nodes and resistance towards susceptible nodes. In 2015, Del Rey *et al.* [40] introduced a CA model the dynamics of which is based on logic transition functions. This model considered smartphone mobility and the heterogeneity of operating systems. However, it did not consider some important scenarios for worm propagation by Bluetooth, such as the interruption of worm transmission due to mobility as devices come in and out of range with each other. González and Lárraga *et al.* [42] proposed a two-dimensional CA-based model to study the propagation of a Bluetooth worm based on epidemiological compartmental models. This research classified each smartphone epidemic state into one of seven types: susceptible, exposed, infected, diagnosed, carrier, interrupted, and recovered. It defined a set of local rules to simulate the dynamics of the model when homogeneous smartphones were considered. More recently, this model was extended to consider the probability of recovering and having an antivirus update and its effects against the worm. However, the described models do not take into account other factors that affect worm propagation, including human behavior, user interaction, malware transmission characteristics and their impact on the propagation dynamics to determine how a Bluetooth malware might spread under different conditions. This research also considers different transmission ranges due to various types of Bluetooth antennas, i.e., with a transmission range of 1, 10, or 100 m, as well as the transmission acceptance and the discoverable mode as a function of the user's direct intervention.

In this paper, the model proposed in [43] is further extended by adding the necessary rules to include new features to better represent real smartphone interactions and communications. The following new features are considered in the definition of the dynamics of the proposed model and its behavior: 1) Different Bluetooth antenna classes were considered that consequently implied different ranges and transmission rates which affect the time to transmit the worm payload; in other words, a worm can propagate faster in some devices; 2) Renewal factors to simulate existing devices moving out of the area under study and new devices moving in; 3) The influence of different types of device mobility. In addition, tuning of input parameters, e.g., transmission rates, worm file size, etc., are adjusted using real data provided by some public reports about antivirus software. The proposed model is useful to represent malware propagation based on operating system vulnerabilities, the appearance of which is difficult to predict. The sheer number of Bluetooth devices in circulation makes studying malware propagation a relevant phenomenon to analyze. Different simulation scenarios were designed to analyze how a Bluetooth worm might spread. The experiments considered the location where the outbreak begins, the user's awareness about the risks inherent while using smart devices in Bluetooth networks, and the different types of antennas integrated into the smart devices. Simulation results indicate that the proposed model is appropriate to study how the user's demographics affect worm propagation in time and space.

The rest of this paper is organized as follows. Section II introduces the proposed model, while Section III presents simulation results obtained from this model under different scenarios. Finally, Section IV introduces the conclusions and some suggestions for future work.

II. WORM PROPAGATION MODEL
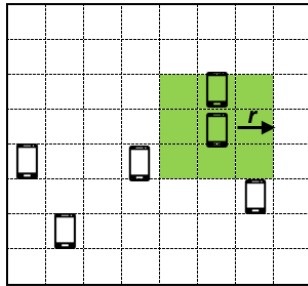### A. CELLULAR AUTOMATA
Cellular automata (CA) are recognized as an intuitive modeling paradigm for Complex Systems. CA are mathematical dynamic system models, that, are spatially and temporally discrete. They are composed by a finite set of cells, each one possibly occupied by agents that evolve in parallel at discrete timesteps. The state of each agent is updated in accordance with a set of dynamic transition rules that takes into account the state of agents in the cells in its neighborhood.

Formally, CA can be defined as a five-tuple, $\{N, \mathcal{C}, \Omega, V, f\}$, where N is the set of individual agents, $\mathcal{C}$ denotes the cellular space, Ω denotes a finite state set the elements of which are all the possible states of the agents, V denotes the cell neighborhood of each agent, and f denotes a set of local transition rules. In particular, for two-dimensional CA, cellular space $\mathcal{C}$ is represented as a regular spatial lattice or grid $\mathcal{C}$ of $L \times M$ cells, $\mathcal{C} = \{(i, j) \mid i, j \in \mathbb{Z}, 1 \leq i \leq L, 1 \leq j \leq M\}$. At time t, each agent stays in one of the finite numbers of possible discrete states in Ω. By interacting with the agents in its neighborhood V, each agent updates its current state following the set of specific transition rules in f.

This CA paradigm forms the basis of the worm propagation model introduced in the following subsection.
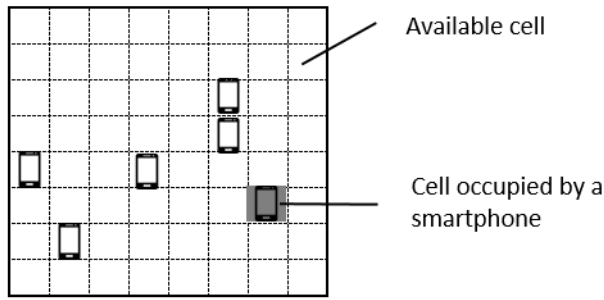
(a) Discretized representation of the geographic space and smartphone positioning.

(b) Modeling of Bluetooth antenna range through using a Moore neighborhood.

FIGURE 1. Cellular space $\mathcal{C}$.

B. THE MODEL

The proposed model is a probabilistic cellular automaton. Agents are N individuals with smartphones randomly deployed on the two-dimensional lattice C, that represents the geographic area under study. Then, each cell has an associated position (i, j), which in this paper represents an area of 1 m^2. Besides, cells can be either empty or occupied by just one individual with a smartphone, as shown in Fig. 1a. Transitions in time are from $t \rightarrow t+1$, which implies the timestep is equal to 1 s.

On the other hand, each smartphone $u \in N$ at location (i, j) can establish contact only with those smartphones within a neighborhood $V(u)_{(i,j)}$ that represents the radial transmission range of a Bluetooth antenna using a 2D Moore neighborhood with radius r, the value of which depends on the class of Bluetooth antenna considered and defined by:

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

as shown in Fig. 1b.

In our model, only two classes of Bluetooth antenna are considered, which are described in [44]: class 2 (10 m of transmission range) and class 3 (1 m of transmission range).

C. SMARTPHONE STATES

The epidemic state of a smartphone is divided according to the propagation dynamics of Bluetooth worms as follows:

a. **Susceptible state (S)**. Denotes devices that have not been infected by another infectious smartphone but are prone to infection.

b. **Exposed state (E)**. Devices that have been in contact with the worm, but are not yet able to spread it to a susceptible smartphone because a complete copy of the worm has not yet been transmitted to them.

c. **Infected state (I)**. Devices that have received a full copy of a worm compatible with its operating system. Therefore, they may infect other susceptible smartphones within their transmission range.

d. **Carrier (C)**. Devices that have received a full copy of the worm payload that it is not compatible with their operating system. Consequently, it is assumed that the worm cannot operate properly and is not capable of continuing to spread. This is a terminal state.

e. **Recovered state (R)**. Devices in which the worm has been removed by applying a factory reset or restoring a backup, giving them temporal immunity. Devices in a Recovered state may also go back to a Susceptible state, representing some devices getting out of the cellular space and new ones coming in, thus keeping the total number N constant.

f. **Interrupted state (INT)**. Denotes exposed devices receiving a copy of the worm that, due to its mobility, went out of the infecting device's transmission range before the transmission of the worm payload finished. This state also encompasses those devices receiving a copy of the worm and the recovery of the corresponding infected smartphone. A device that has reached this state will go back to a Susceptible state at the next timestep.

The infection state for the smartphone u located at position (i, j), at timestep t is denoted by $\omega_{ij}^u(t)$, in which $\omega_{ij}^u(t) \in$ {S,E,C,I,R,INT}. Let the number of susceptible, exposed, carriers, infectious, and recovered devices at time t be denoted by $S(t)$, $E(t)$, $C(t)$, $I(t)$, $R(t)$, and $INT(t)$, respectively. Then, $N = S(t) + E(t) + C(t) + I(t) + R(t) + INT(t)$, implying that N, the number of smartphones in the cellular space $\mathcal{C}$ remains constant throughout the simulation time.

D. SMARTPHONE ATTRIBUTES

Each agent in the cellular space $\mathcal{C}$ is a smartphone provided with attributes of real devices, the value of which is stored in the individual variables described in Table 1. Initially, smartphones are randomly deployed on the cellular space with a probability P_{MOV} to start moving randomly. At each timestep, a smartphone could move from its current position (i, j) to any available adjacent cell in its neighborhood.

The state of each smartphone in $\mathcal{C}$ will change at each timestep, according to a set of local rules represented by the transition diagram depicted in Fig. 2. Here, $f_{T_{SE}}(u)$, $f_{T_{EINT}}(u)$, $f_{T_{EI}}(u)$, $f_{T_{EC}}(u)$, and $f_{T_{EE}}(u)$ are logical functions that a smartphone uses to change its state from state S to E, E to INT, E to I, E to C, and E to E, respectively. Besides, a smartphone in the state I will transition to state R if the probability P_{IR} is met. Otherwise, it will remain in state I. Finally, if P_{RS} is met, then the smartphone in state R will transition back to state S. The following subsection details the rules that define the transitions between states.

TABLE 1. Attributes of a smartphone agent *u* at time *t*.

Attribute	Description
os	Type of operating system installed on the smartphone (Android or other)
$\omega_{ij}^{u}(t)$	Current state of the smartphone at time t. Transition functions will use this value to calculate the next state.
$\omega_{ij}^{u}(t+1)$	State to which the smartphone will transition to at timestep $t+1$
IST	Infection start time. Timestep where a smartphone transitioned to state E. The value of this attribute's value will be considered in $t+1$, because the incoming connection must be accepted before starting transmission.
$U_{u_{BT}}^{t}$	Logical variable indicating if the Bluetooth antenna is on
D_{u}^{t}	Logical variable indicating if the Bluetooth antenna is on discoverable mode
$A_{u_{acc\_v}}^{t}$	Logical variable indicating that the owner of the smartphone u accepts the incoming transmission from a neighbor smartphone v at time t
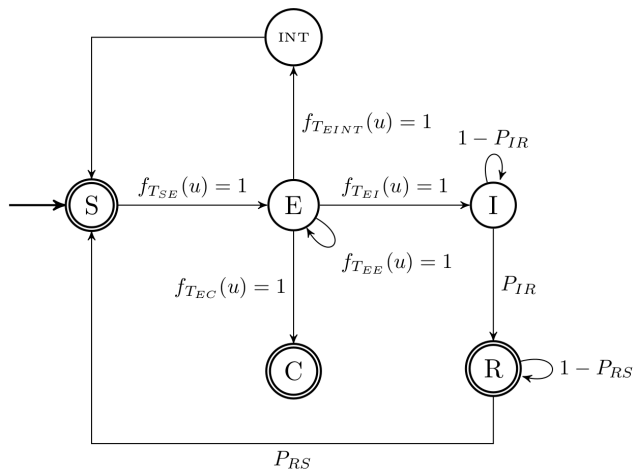
FIGURE 2. State transition diagram of an arbitrary smartphone.

E. TRANSITION BETWEEN STATES

In order to describe the phases of the worm spreading through Bluetooth antennas, the model considers the following rules to control its evolution:

a. **From a Susceptible to an Exposed State**. This transition represents the situation in which the owner of a healthy smartphone accepts the transmission of an infected smartphone in its neighborhood, signaling that the infection can start. For this to happen, four conditions must be met: 1) The probability to be infected by a nearby infectious smartphone; 2) The Bluetooth antenna must be turned on; 3) The antenna must be on discoverable mode; and 4) The user must accept the incoming transmission. Consequently, the logical function used to determine the transition from a Susceptible to an Exposed state is described as follows:

$$f_{T_{SE}}(u) = X_{p_i}^{t} \wedge U_{u_{BT}}^{t} \wedge D_{u}^{t} \wedge A_{u_{acc\_v}}^{t} \quad (1)$$

with

$$X_{p_i}^{t} = \begin{cases} 1 & \text{with probability } P_{Contagion} = \beta \frac{I_u(t)}{N_u(t)} \\ 0 & \text{with probability } 1 - P_{Contagion} \end{cases} \quad (2)$$

$$U_{u_{BT}}^{t} = \begin{cases} 1 & \text{with probability } P_{BT} \\ 0 & \text{with probability } 1 - P_{BT} \end{cases} \quad (3)$$

$$D_{u}^{t} = \begin{cases} 1 & \text{with probability } P_{D} \\ 0 & \text{with probability } 1 - P_{D} \end{cases} \quad (4)$$

$$A_{u_{acc\_v}}^{t} = \begin{cases} 1 & \text{with probability } P_{acc} \\ 0 & \text{with probability } 1 - P_{acc} \end{cases} \quad (5)$$

where $u \in N$ is the smartphone in cell location (i, j), $N_u(t)$ is the total number of neighboring smartphones of u at time t, $\beta \in [0, 1]$ is the infection rate, according to [25], and $I_u(t)$ is the total number of infected smartphones in u neighborhood at time t. Thus, $X_{p_i}^{t}$ is the logical variable that indicates whether a smartphone could be infected from a worm transmitted by a nearby infectious smartphone. $U_{u_{BT}}^{t}$ is a logical variable that indicates whether the antenna of smartphone u is on at time t with probability P_{BT}. D_{u}^{t} indicates whether the antenna of smartphone u is on discoverable mode at time t with a probability P_{D}. Finally, $A_{u_{acc\_v}}^{t}$ also takes a logical value that indicates whether the owner of the smartphone u accepts the incoming transmission from a neighboring smartphone v at time t with a probability P_{acc}. Consequently, the transition from a Susceptible to an Exposed state is given as follows;

$$\omega_{ij}^{u}(t+1) = \begin{cases} E, & \omega_{ij}^{u}(t) = S, f_{T_{SE}}(u) = 1 \\ S, & \omega_{ij}^{u}(t) = S, f_{T_{SE}}(u) = 0 \end{cases} \quad (6)$$

b. **From an Exposed to an Infected, or from an Exposed to an Interrupted, or from an Exposed to a Carrier State**. This state transition represents what happens to an exposed smartphone that is already in contact with an infected one. Three possible events may occur: 1) The exposed and infected smartphones remain in transmission range r for a latency time LT until the worm is sent and both devices have the same operating system; 2) The exposed and infected smartphones interrupt transmission by going out of range r before the latency time LT is completed; and 3) The infected smartphone completes worm transmission in time LT, however, the receiving smartphone has a different operating system than the one targeted by the worm. In order to clarify this transition, suppose that at time t cell (i, j) is occupied by the smartphone of interest u with current state E denoted as $\omega_{ij}^{u}(t) = E$ that will evolve at time $t+1$ to state C, I or INT according to the following conditions:

$$\omega_{ij}^{u}(t+1) = \begin{cases} E, & \omega_{ij}^{u}(t) = E, f_{T_{EE}}(u) = 1 \\ INT, & \omega_{ij}^{u}(t) = E, f_{T_{EINT}}(u) = 1 \\ I, & \omega_{ij}^{u}(t) = E, f_{T_{EI}}(u) = 1 \\ C, & \omega_{ij}^{u}(t) = E, f_{T_{EC}}(u) = 1 \end{cases} \quad (7)$$

TABLE 2. Example of exposed smartphones attributes.

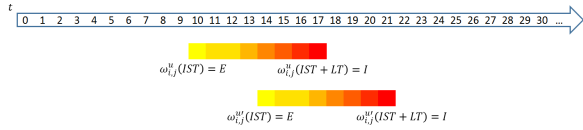| Smartphone u		
📱	osType	Android
	Current state	Exposed
	IST	10
Smartphone u'		
📱	osType	Android
	Current state	Exposed
	IST	14

FIGURE 3. Timeline in the transition from exposed to infected state assuming a latency time LT = 7 s.

where $f_{T_{EE}}(u)$, $f_{T_{EINT}}(u)$, $f_{T_{EI}}(u)$ and $f_{T_{EC}}(u)$ are logical functions that a smartphone uses to change its state from state E defined as follows:

$$f_{T_{EE}}(u) = \begin{cases} 1 & t < \Delta t \wedge v_I \in V_u \\ 0 & \text{otherwise} \end{cases} \quad (8)$$

$$f_{T_{EINT}}(u) = \begin{cases} 1 & t < \Delta t \wedge (v_I \notin V_u \vee U^t_{BT_u} = 0) \\ 0 & \text{otherwise} \end{cases} \quad (9)$$

$$f_{T_{EI}}(u) = \begin{cases} 1 & t \geq \Delta t \wedge v_I \in V_u \wedge u_{os} = v_{I_{os}} \\ 0 & \text{otherwise} \end{cases} \quad (10)$$

$$f_{T_{EC}}(u) = \begin{cases} 1 & t \geq \Delta t \wedge v_I \in V_u \wedge u_{os} \neq v_{I_{os}} \\ 0 & \text{otherwise} \end{cases} \quad (11)$$

Here, V_u represents the neighborhood of smartphone u. $v_I \in V_u$ denotes the infected device that is transmitting the worm to the smartphone u at timestep t. u_{os} and $v_{I_{os}}$ are used to denote the type of smartphone's operative system of devices u and v_I, respectively. Δt represents the time required for the infection to be completed, defined as $\Delta t = IST + $ LT; in which *IST* represents the infection starting time and LT the latency time.

To illustrate this case, consider two different smartphones denoted as u and u', respectively, the attributes of which are shown in Table 2. Let's assume that both smartphones accept the worm transmission of an infected smartphone in its neighborhood and change from a Susceptible to an Exposed state at time $t = 10$ and $t = 14$, respectively. Fig. 3 depicts their evolution over time, in which can be observed that smartphones u and u' become infected at time $t = 17$ s and $t = 21$ s, respectively.

c. **From an Interrupted to a Susceptible State**. This state transition represents the situation in which a smartphone was connected to an infected device and one of the two devices left the range of the Bluetooth antenna before worm transmission ended. Therefore, the connection is assumed to have been interrupted. Consequently, the exposed smartphone does not have a full copy of the worm, so it is not affected by it and thus returns to a

Susceptible state. Assuming that smartphone u is located at cell (i, j) and its current state is INT denoted as $\omega^u_{ij}(t) = $ INT, then the state will unconditionally evolve to state S at the next timestep, as shown in (12).

$$\omega^u_{ij}(t + 1) = S \quad (12)$$

d. **From an Infected to a Recovered State**. This state transition represents an infected smartphone owner's attempt to recover the device by restoring a backup or by a factory reset. Let us suppose that smartphone u is located at cell (i, j) and its current state is I, denoted as $\omega^u_{ij}(t) = $ I; this will evolve to the state R if probability P_{IR} is met, which indicates that the attempt to remove the worm from the operating system was successful; otherwise, the device will remain in the state I. The transition occurs as follows:

$$\omega^u_{ij}(t + 1) = \begin{cases} R, & \omega^u_{ij}(t) = \text{I with probability } P_{IR} \\ I, & \omega^u_{ij}(t) = \text{I with probability } 1 - P_{IR} \end{cases} \quad (13)$$

e. **From a Recovered to a Susceptible State**. This state transition simulates new smartphones entering the cellular space, whereas existing smartphones are moving out of it, with a probability P_{RS}, always keeping N unchanged. Suppose that a smartphone u is located at cell (i, j) and its current state is R, denoted as $\omega^u_{ij}(t) = R$; then, this will evolve to state S if probability P_{RS} is met. This transition is represented as follows:

$$\omega^u_{ij}(t + 1) = \begin{cases} S, & \omega^u_{ij}(t) = \text{R with probability } P_{RS} \\ R, & \omega^u_{ij}(t) = \text{R with probability } 1 - P_{RS} \end{cases} \quad (14)$$

F. MOBILITY DYNAMICS

The proposed model introduces smartphone mobility throughout cellular space $\mathcal{C}$, an important factor in the infection process by Bluetooth. Every smartphone can thus move to one of the nearest available cells into a Moore neighborhood at each timestep, provided that movement probability P_{MOV} is met, as shown in Fig. 4. Three different types of movements are considered:

a. Straight Line (SL). A smartphone will continue to move in the same direction with probability P_{MOV} if and only if another smartphone does not already occupy the target cell or the target cell is located on the border of the cellular space. Otherwise, the smartphone will remain in its origin cell, and a new direction will be assigned at the next timestep (see Fig. 5a).

b. Random Walk (RW). A smartphone will move to a randomly selected direction at each timestep with a probability P_{MOV} if and only if another smartphone does not already occupy the target cell or the target cell is not on the border. Otherwise, the smartphone will remain still (see Fig. 5b).

c. Mixed Movement with Pauses (MMwP). A smartphone will move with a probability P_{MOV}, according to the following steps

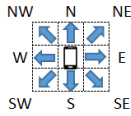**FIGURE 4.** Moore neighborhood used to assign the motion direction of smartphones.

TABLE 3. General input parameters and variables.

Parameters	Description
β	Infection rate
LT	Latency time
P_{MOV}	Probability of movement
P_{IR}	Probability of recovering an infected smartphone
P_{RS}	Probability that a smartphone in a Recovery state evolves to Susceptible state
P_{BT}	Probability that the antenna of a smartphone is on at time t
P_{acc}	Probability that a smartphone accepts the worm transmission from an infected device at time t.
P_D	Probability that a smartphone is on discoverable mode at time t

a) A time frame is assigned with a duration between [1,5] seconds.

b) A movement pattern is assigned (SL, RW or a pause).

c) The movement is executed, using the assigned time frame and pattern.

d) The first three steps are repeated until simulation ends.

This movement is depicted in Fig. 5c.

Table 3 contains a summary of the parameters of the proposed model.

G. GENERAL CONSIDERATIONS REGARDING THE PROPOSED MODEL

This subsection summarizes considerations for the proposed model, as they are important for an understanding of its dynamics and behavior.

- This model considers Bluetooth connections as an infection vector only. Bluetooth stack and other Bluetooth low-level features are out of the scope of this research.
- Smartphones may have different characteristics or configurations, which influence how the worm spreads (operating systems and security settings).
- The operating systems considered in this model are Android and others.
- The infection dynamics considers that an infected smartphone can attack susceptible ones within its transmission range.
- To complete the infection, the susceptible and infected smartphones must stay within the transmission range throughout all the latency time.
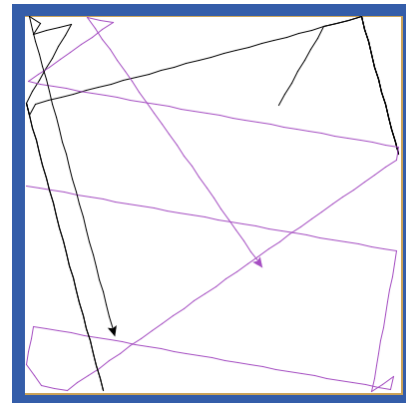
(a) Straight Line Pattern.
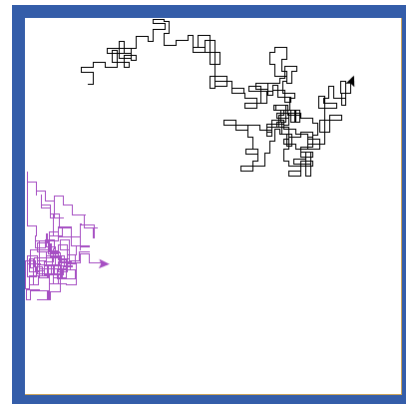
(b) Random Walk Pattern
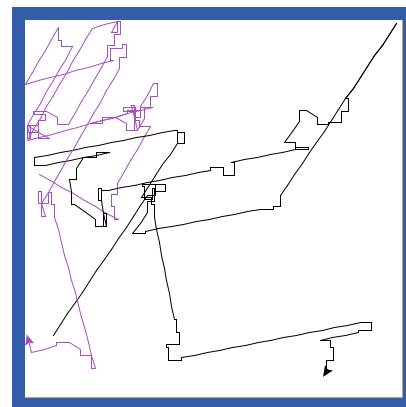
(c) Mixed Movement with Pauses Pattern.

FIGURE 5. First 200 timesteps of two smartphones using the three different motion models. The point of the arrow corresponds to the direction of movement.

- An infected device can be connected to at most one exposed smartphone at a time and vice versa.
- In case an infected smartphone connected to another one is recovered as a result of the recovery process, then it will be disconnected from the exposed device, putting an end to the whole infection processes.
- Exposed smartphones that became connected to an infected smartphone that was eventually recovered will transition to an INT state due to the cancellation of the infection process.

- The motion model considers that a smartphone can move one cell at each timestep to represent that the device holder is walking.
- Smartphones in an INT state will unconditionally go back to a susceptible S state at the next timestep.
- The model evolves in timesteps t equal to 1 second.
- It is assumed that the worm modeled in this research attacks Android devices only.

III. SIMULATION RESULTS AND DISCUSSION

This section presents simulation results from the proposed model in order to evaluate the propagation dynamics of Bluetooth worms in smartphones. For this purpose, it includes three sets of results. The first two analyze the effect of key factors in a worm infection, such as: latency time, initial position of infected devices, range of Bluetooth antennas, and rates of recovery and renewal. Each one of these factors is analyzed for a range of smartphone densities in cell space (see Subsections III-B and III-C). The third set of results illustrates how dynamics are affected by user choices, such as turning the antenna on, putting the device in discoverable mode, or accepting an incoming transmission. All of these choices are made versus different values of smartphone density (see Subsection III-D). Figure 6 shows a flowchart that summarizes the simulation steps of the model introduced in this work.

A. GENERAL SCENARIO

For all cases, simulations are carried out on a 2D lattice $\mathcal{C}$ of 101×101 cells, which represents a typical limited geographic space in an urban area. Each cell represents an area of 1 m^2 and can be occupied or not by a smartphone at time instant t. Besides, as already mentioned in the previous section, a Moore neighborhood is considered for each cell in position (i, j)

All simulation results presented in the first set of results were generated by simulations of 21,600 s (6 hours). For each smartphone density value considered, 10 simulation runs were made and the obtained results averaged. All tests considered a heterogeneous population of smartphones in which 84% are Android devices. It is also assumed that the worm modeled in this research attacks Android devices only. Moreover, for all simulation results, density of smartphones σ, which is defined as $\sigma = N/(101 \times 101)$ varies from 0.1 to 0.9, with steps of 0.1, unless otherwise stated.

Besides, an infection rate β with a value of 0.9 was considered in order to simulate a very aggressive worm that allows for an analysis of the role model parameters play in propagating the infection. Moreover, the corresponding value for the movement probability P_{MOV} is maintained at 0.1 for all of the experiments, trying to reproduce a slow motion speed within the cell space. The rest of the parameters will be described in each case study. Simulations results are carried out by using Netlogo 5.1.0, a programmable modeling environment developed on the programming languages Scala
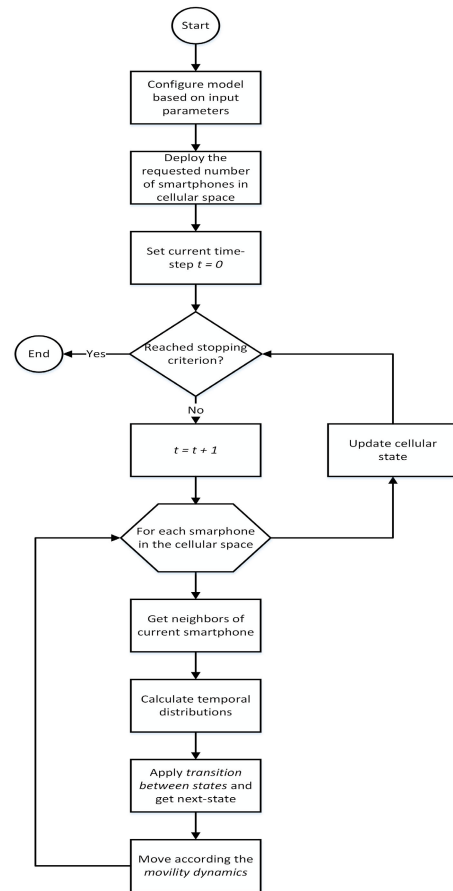

FIGURE 6. Flowchart of the proposed model simulation steps.

and Java for simulating complex systems developing over time as the model introduced in our manuscript.

B. THE IMPACT OF PHYSICAL PARAMETERS ON MALWARE PROPAGATION

This subsection collects controlled experiment results, based on varying key factors in order to determine their impact on malware propagation. In particular, simulation results were obtained through varying latency time, the infected devices' initial position, and Bluetooth range.

For all simulation results in this subsection, in order to explore the impact of physical parameter variation on malware propagation, it was assumed that devices had their antennas on, were in discoverable mode, and were accepting all transmission requests, i.e., $P_{BT} = P_D = P_{acc} = 1$.

1) LATENCY TIME

The amount of time a worm needs to self-propagate to other susceptible smartphones nearby using Bluetooth is related to latency time, which depends on the worm's file size and Bluetooth's transmission data rate. Thus, as the initial point of the research, the dynamics of malware spreading were analyzed through varying the Bluetooth data rate, which directly affects the latency time required to complete the worm payload transmission to other devices, using different smartphone

density values. In particular, data rates of 1 Mbps, 2 Mbps, and 3 Mbps were considered [44]. Besides, according to [45]–[49], there is no standard size for malicious software. However, the trend is that small sizes are preferred due to the shorter time required to transmit them over the network. Thus, in this research a hypothetical malware file size of 1 MB (1024 KB) was assumed. By taking into account this malware size and considering the three transmission rates, latency time LT = 8, 4, and 2.67 s, for data transfer rates of 1 Mbps, 2 Mbps, and 3 Mbps, respectively, were obtained as follows:

$$LT = \frac{\text{file size}}{\text{transfer rate}} \quad (15)$$

Thus, five different scenarios were analyzed. Three of them resulted from LT = 2.67, 4, and 8 s; the fourth one used a variable transmission rate, denoted as LT_x such that, on the basis of a discrete uniform distribution, at each timestep one of the three latency times is chosen. Finally, the fifth scenario considered latency time to be the average of the three transmission rates, i.e., LT = 4.89 s. For all the simulations, and given a density σ, the initial position of smartphones in cell space $\mathcal{C}$ was randomly assigned. Besides, initially 10% of devices were considered to be in an infectious state I. This random placement allows no other factors to interfere in the dynamics of the infectious process, such as the starting position of the smartphones (presented later on). Moreover, no renovation and renewal effects were considered, that is, $P_{IR} = 0$ and $P_{RS} = 0$, respectively.

Fig. 7a shows the variation of the time required by the worm to infect all the smartphones with an Android operating system (84% of the total population) for the first four scenarios of LT = 2.67, 4, 8, and LT_x s, when different density values of σ are considered. As can be observed from this figure, the larger the latency time value, the more time is required to infect the entire population, as occurs in reality. On the other hand, note that this required time becomes shorter as density increases because the probability that a user moves is smaller, therefore increasing the probability of infection as the device remains within the antenna range of an infected device for a longer time. Therefore, higher density has a larger influence than latency time in worm propagation.

Besides, Fig. 7b compares the fourth and fifth scenarios, demonstrating that the obtained behavior for LT = LT_X s is very similar to that corresponding to LT = 4.89 s, the average of the three latency values considered. Based on these last results, in the rest of the simulation experiments, a LT = 4.89 s will be used.

2) INITIAL POSITION OF INFECTED DEVICES
In models of propagation of biological viruses, infectious outbreaks are simulated through the appearance of a single infected individual at time $t = 0$, from which subsequent contagions will occur. Thus, the following experiments are meant to study how the initial position of the infected
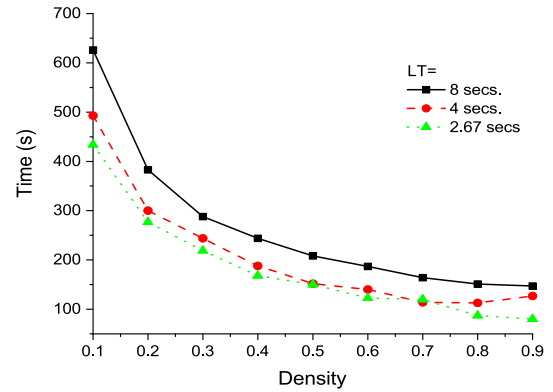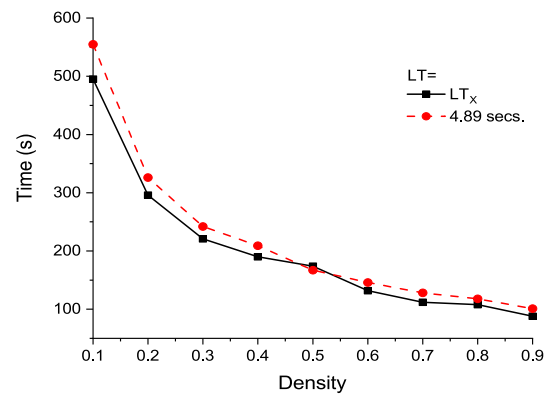

(a) LT = 2.67, 4 and 8 s.

FIGURE 7. Time required to complete worm propagation versus smartphone population density, using $P_{MOV} = 0.1$, $P_{IR} = 0$ and $P_{RS} = 0$, $P_{BT_1} = 1$, $\beta = 0.9$ and different latency times LT.

smartphone influences the time evolution of the worm's propagation to other devices within its transmission range in order to determine the spatial conditions that favor or impair the infection dynamics. For this, two different initial positions of the infected smartphone were considered because of the symmetry of the geometrical area: in a corner and at the center of the space. For both initial positions, results were obtained through considering two different types of motion patterns (see subsection II-F): Straight Line (SL) and Random Walk (RW).

Figures 8a and 8b show the time evolution of the proportion of infected smartphones when the initial position of the infected smartphone is at the center of the geographic space, for SL and RW movement patterns, respectively. It can be observed that a faster worm propagation occurs for the SL pattern if density is low, $\sigma \leq 0.5$. However, when density is high, $\sigma > 0.5$, the worm propagation evolves slightly faster for the RW movement pattern (see the insert in figure). This occurs because the SL pattern tends to move across larger routes than RW, which moves locally. Similar qualitative behavior occurs when the initial position of the infected smartphone is placed in a corner of cell space $\mathcal{C}$ and is not shown for economy of space.
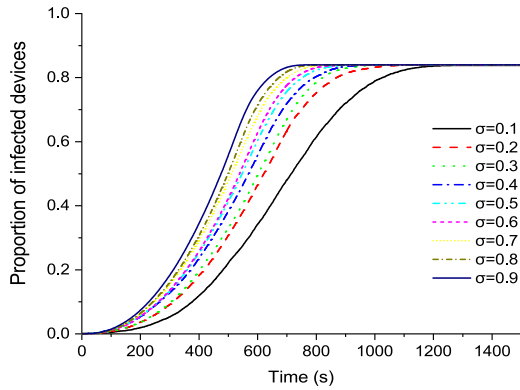
(a) Center, Straight Line.
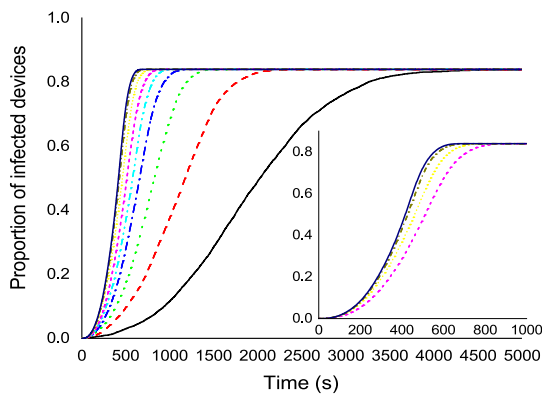
(b) Center, Random Walk.

FIGURE 8. Proportion of infected vehicles with respect to time, for different density values, when the initial position is set at the center of the geographic space. a) Straight line (SL) movement; b) Random walk (RW) movement. All devices had their antennas on, were in discoverable mode, and were accepting all transmission requests, i.e. $P_{BT} = P_D = P_{acc} = 1$.

Results are summarized in Figs. 9a and 9b, that correspond to the time required for the worm to infect all the smartphone population against density σ, for both SL and RW movement patterns, when the infection starts at the center or corner of cell space $\mathcal{C}$, respectively. Note that the observed behavior is qualitatively similar, regardless of the initial position of the first infected device. However, the combination of the infected smartphone's initial position and the type of movement quantitatively affects the outbreak in terms of time. In particular, the time required when the infection starts from a corner is about 40% longer than when it starts from the center. This can be observed more clearly in Fig. 10 that shows the spatial-time state of the system after 500 s for both initial positions. Fig. 10a shows the state of the system when the infection starts at the center, whereas Fig. 10b shows the state of the system when the infection starts at a corner. Note that the position in the center of the cellular space greatly favors the worm's propagation speed and constitutes the worst scenario to estimate the impact of worm propagation in a limited space.
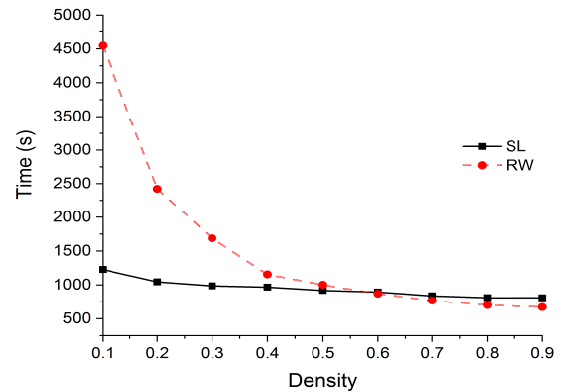
(a) Infection started from center.
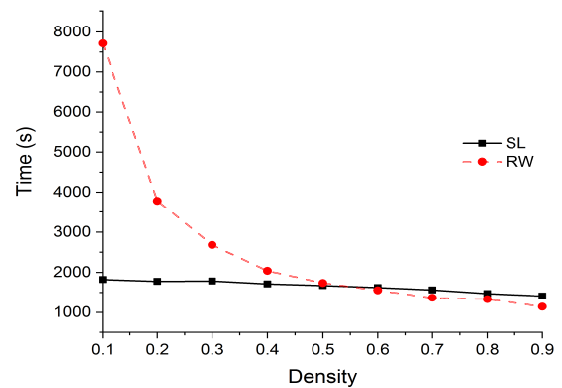
(b) Infection started from a corner.

FIGURE 9. Comparison of the time for complete worm propagation versus smartphone population density considering multiple movement patterns.

### 3) RANGE OF BLUETOOTH ANTENNAS

As mentioned earlier, derived from its lack of centralized security infrastructure, Bluetooth has serious security vulnerabilities that can expose important information on a device to others on Bluetooth networks. Thus, this sub-subsection analyzes worm propagation for Bluetooth antenna ranging 1 and 10 m (see [42] for a description of the standard) in order to evaluate impact. Simulation scenarios started by using only the 1 m range antennas and gradually increased the number of devices with 10 m range. The proportion of the smartphone population with each type of antenna range was indicated with variables P_{r1} and P_{r10}, such that $P_{r1} + P_{r10} = 1$. The latency time used for these experiments was the average value of 4.89 s calculated in subsection III-B1.

Based on the results of previous sections, simulations were made only when the infection started at the center of cell space $\mathcal{C}$ and with straight-line motion patterns.

Figures 11a and 11b show the time evolution of the proportion of infected devices, for different values of device density in cell space $\mathcal{C}$, when two scenarios of antenna distribution are considered: a) $P_{r1} = 0.5$ and $P_{r10} = 0.5$ and b) $P_{r1} = 0$ and $P_{r10} = 1$. Several aspects should be noted in these figures.
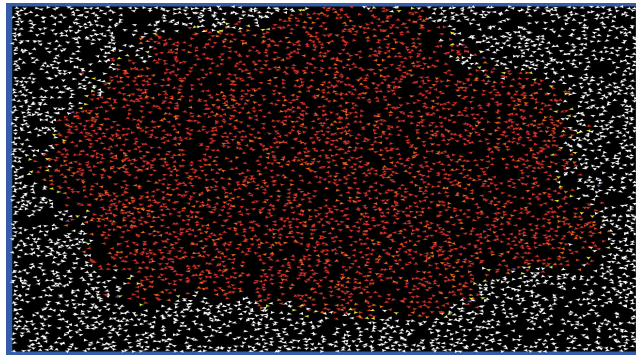
(a) Center, $t = 500$ s.
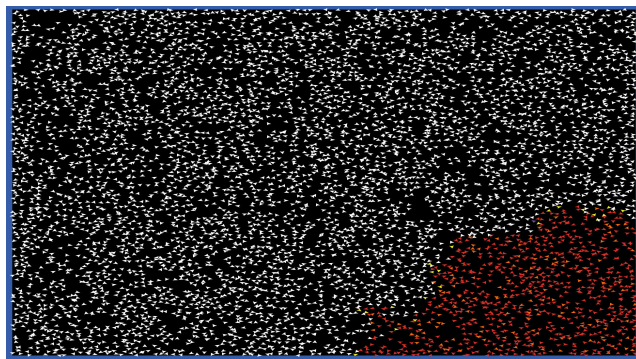
(b) Corner, $t = 500$ s.

FIGURE 10. Spatial-temporal diagrams of the evolution of infection at timestep 500 s.
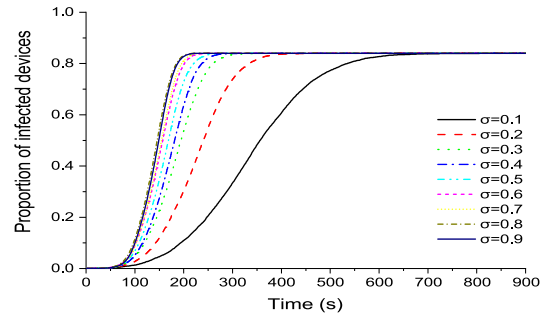

(a) $P_{r_1} = 0.5, P_{r_{10}} = 0.5$.

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

FIGURE 11. Time evolution of the infection versus smartphone population density considering different ranges for Bluetooth antennas, first infected device is placed at the center of the cell space $\mathcal{C}$ and SL movement is considered.
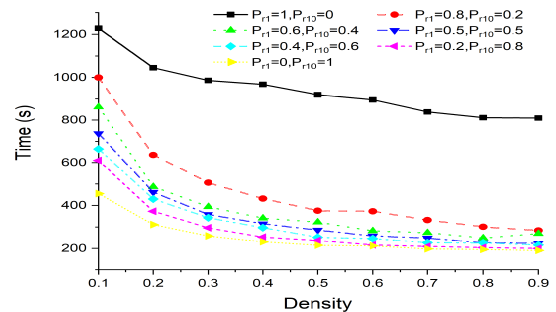

FIGURE 12. Time evolution of the infection versus smartphone population density considering different ranges for Bluetooth antennas, the infected device is first placed at the center of cell space C and SL movement is considered.

First, the speed of worm propagation is faster as $P_{r10} \to 1$, since the time to reach full propagation is about 30 % faster when $P_{r10} = 1$; second, note that when density σ is larger than 0.3, time for full worm propagation is very similar for the two scenarios. This clearly indicates a critical value of density, $\sigma > 0.3$, beyond which full spreading cannot be avoided.

In Fig. 12, the time for full worm propagation is plotted against device density for six different combinations of P_{r1} and P_{r10}. Note that when $P_{r10} > 0.4$ and $\sigma > 0.3$, full worm spread takes less than 400 s, or 7 minutes. Only when all antennas have $r = 1$, is the time for full propagation significantly longer. Since range in newer Bluetooth devices tends to be greater, i.e., $r \geq 10$, simulations demonstrate the risk of full worm propagation even for modest values of smartphone density $\sigma \geq 0.3$, if the proportion of devices with greater range exceeds 40%.

C. RECOVERY AND RENEWAL OF INFECTED DEVICES

1) RECOVERY FACTOR

So far, all experiments show worm propagation in a Bluetooth network in which no smartphone has a recovery mechanism. Evidently, this situation does not necessarily reflect reality, since some users may have a backup of their smartphone's personal settings or are simply comfortable resetting their smartphone to factory settings. In order to describe the likelihood of having the malware removed if a smartphone gets

infected, experiments in which the recovery probability, P_{IR}, assumed values larger than zero were carried out and analyzed. In particular, values of $P_{IR} \in [0.01, 0.1]$ were considered.

For all simulation results presented, it was assumed that all devices used a Bluetooth antenna with a range of 10 m, because this is the most common setting for commercial devices (smartphones, tablets, etc.), as described in [44]. Besides, an initial density of infected devices corresponding to 10% of the total devices was considered.
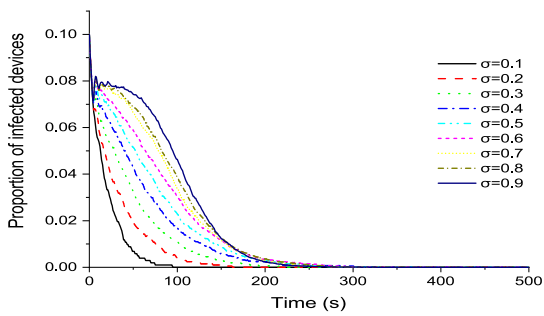
Figure 13 shows the time evolution of the proportion of infected devices depending on smartphone density σ, for four different values of the probability to recover P_{IR}, when SL
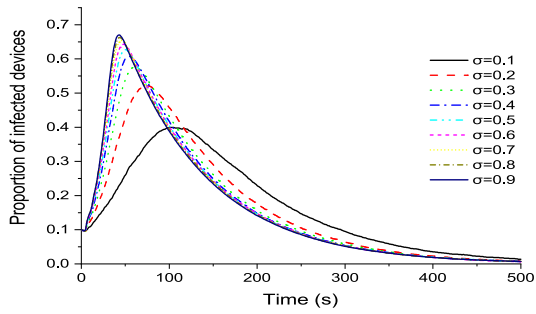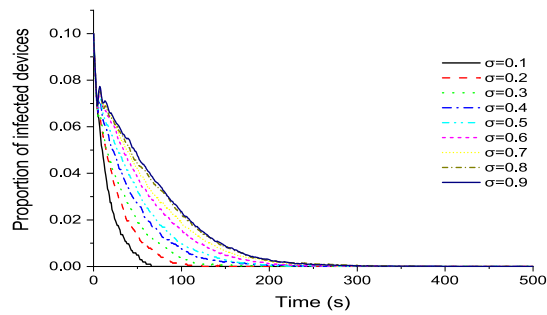
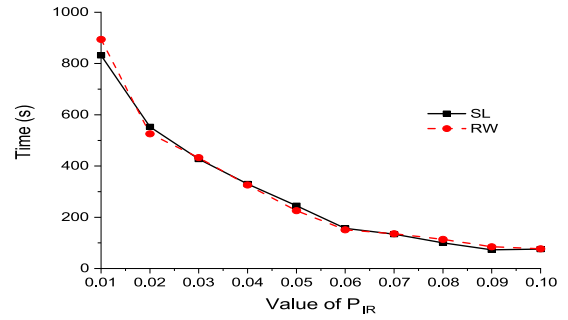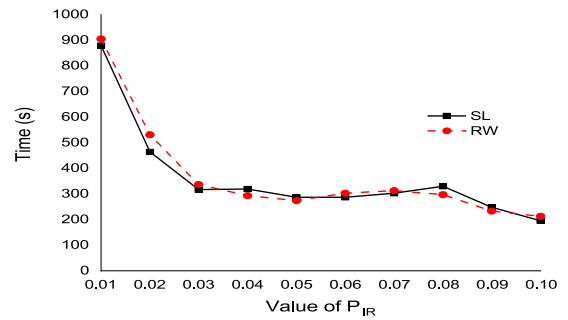(a) $P_{IR} = 0.01$.
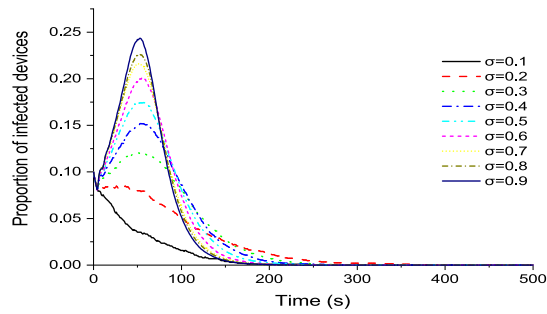
(b) $P_{IR} = 0.05$.

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

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

FIGURE 13. Proportion of infected devices as a function of time, for different values of device density σ and variations in the probability of recovery P_{IR}.
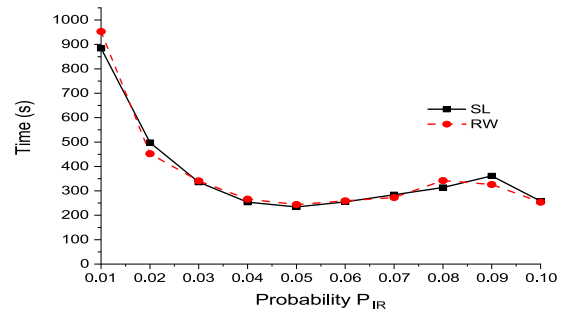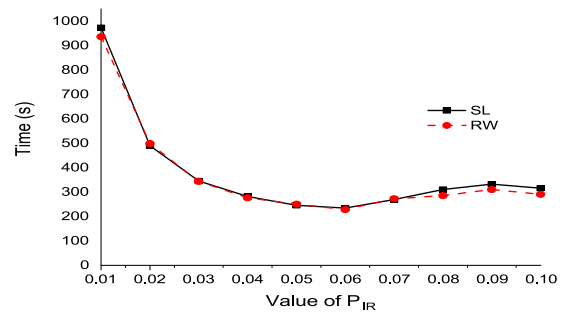

(a) $\sigma = 0.1$.

(b) $\sigma = 0.5$.

(c) $\sigma = 0.8$.

(d) $\sigma = 0.9$.

FIGURE 14. Time to remove the worm from the initial 10% of infected devices versus probability of recovery P_{IR}, movement patterns SL, RW and different density values σ.

motion is used. Plots indicate that in the four cases, all devices eventually recovered, independent from density σ. However,

there are interesting differences between the scenarios. While for lower values, $P_{IR} = 0.01, 0.05$, there is an initial peak in which the propagation exceeds the initial 10% of the

infected population that later in time evolves to eliminate the worms in all devices. On the other hand, for larger values, $P_{IR} = 0.08, 0.09$, there is not an initial peak and the worm is gradually removed. This behavior signals that even modest values, $P_{IR} = 0.01$, can prevent worm propagation.

Simulations are reorganized in Fig. 14, that shows the time it takes to remove the worm compared with different values of P_{IR}, for four values of smartphone density σ and two movement patterns, SL and RW. This figure indicates that there is not a significant difference in the recovery of infected devices due to the movement pattern. Similarly, there is a minimum time to remove the worm from the initially infected devices for each value of σ, time that increases with density σ as there are more devices from which to remove the worm.

2) RENEWAL FACTOR

The aim of this group of simulations is to study the effect of an infection when it becomes endemic, a situation that occurs when the worm cannot be erased entirely from cell space $\mathcal{C}$. Since smartphones can move around this space, probability P_{RS} is introduced to represent that some smartphones can come out of cell space $\mathcal{C}$ and other devices can also come in. Smartphones that leave the cell space are assumed to be in are covered state R, while those entering are in a susceptible state S. The parameters used for these simulations are equal to those used in the previous section.

Figure 15 shows the time evolution of the proportion of infected devices for four different scenarios. In the first three, $P_{IR} = 0.01$ and $P_{RS} = 0.01, 0.05$, and 0.09, respectively, while in the fourth one, $P_{IR} = 0.09$ and $P_{RS} = 0.01$. Figures 15a-15c indicate that for all values of σ the worm cannot be removed from cell space $\mathcal{C}$. The final value of infected devices increases with P_{RS}, as new devices in a susceptible state S can always be infected. Note that for $P_{RS} \geq 0.05$ and $\sigma > 0.1$ infection propagates to all infectable devices. The last plot, in Fig. 15d shows that, with high values of recovery, $P_{IR} = 0.09$ (implying that a high percent of infected smartphone population recovers) and modest values of renewal, $P_{RS} = 0.01$, can still produce an endemic situation, even though the proportion of infected devices is much lower. These simulations indicate the persistence of the infection, even in the face of recovery and renewal mechanisms.

Figure 16 shows the time evolution of the five compartments of interest in the infection-renewal dynamics: S, E, I, R, C. For the sake of simplicity, only σ values 0.1, 0.5, 0.8, and 0.9 are shown, using probabilities $P_{IR} = 0.01$ and $P_{RS} = 0.01$. For a low density, $\sigma = 0.1$, as shown in Fig. Fig. 16a, there are still susceptible devices, although in a smaller proportion. In all the other densities, shown in Figs. 16b-16d, the worm infected all possible devices, and all five states reached similar final values. It is clear that this happens because $P_{IR} = P_{RS}$, which induces a balance
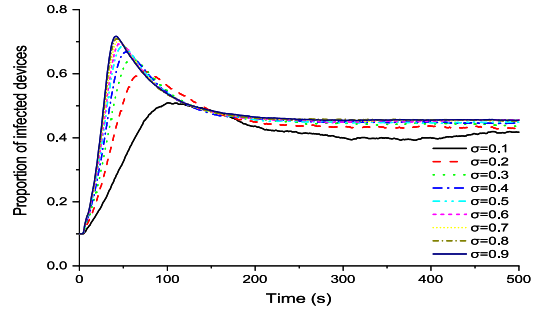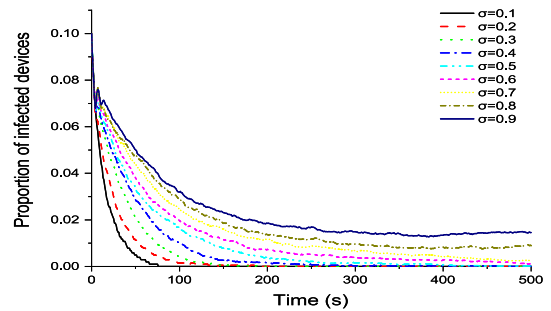

(a) $P_{IR} = 0.01, P_{RS} = 0.01$.
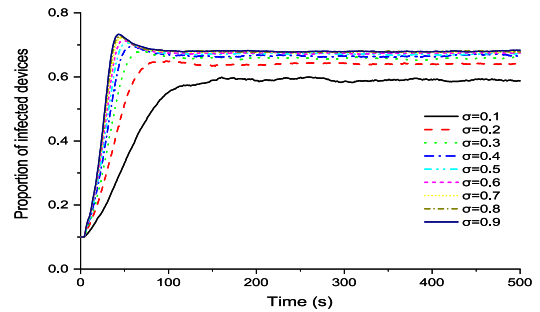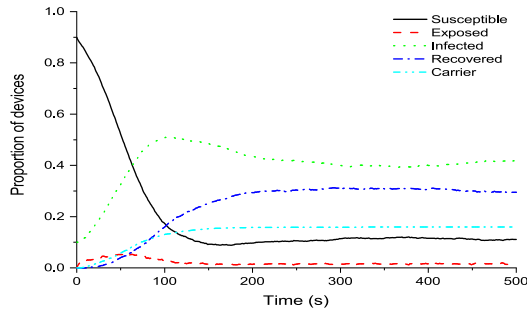

(b) $P_{IR} = 0.01, P_{RS} = 0.05$.
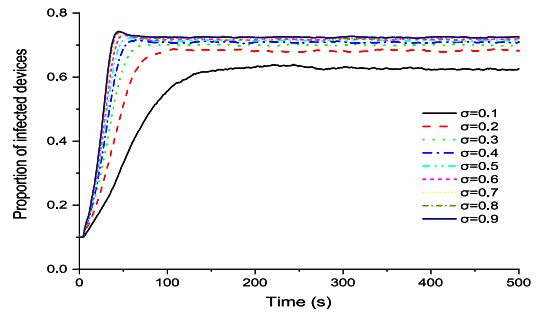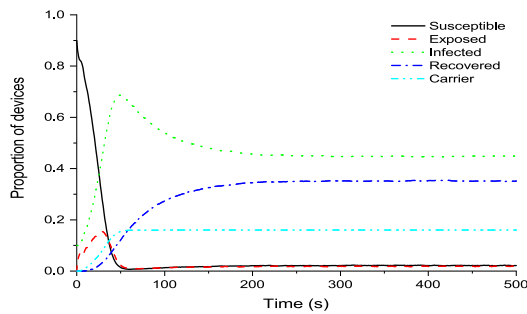

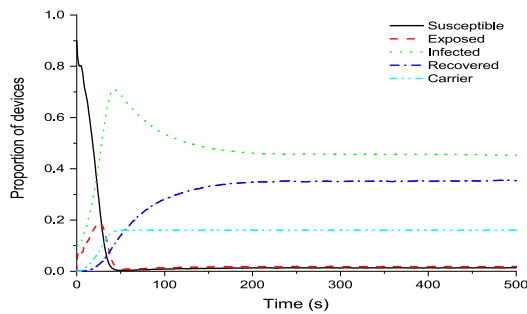(c) $P_{IR} = 0.01, P_{RS} = 0.09$.

(d) $P_{IR} = 0.09, P_{RS} = 0.01$.

FIGURE 15. Evolution of proportion of infected devices on time as a function of the recovery probability P_{IR} and the renewal probability P_{RS}.
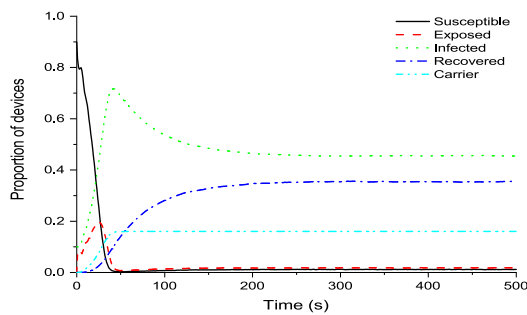
(a) $\sigma = 0.1$.

(b) $\sigma = 0.5$.

(c) $\sigma = 0.8$.

(d) $\sigma = 0.9$

FIGURE 16. Evolution in time of the proportion of susceptible S, exposed E, infected I, carrier C, and recovered R devices for $P_{IR} = 0.01$, $P_{RS} = 0.01$ versus multiple values of density σ.

between new susceptible devices and their transitions to the other terminal states.

D. USER INTERVENTION

Simulation results presented in previous subsections allowed to explore the general worm propagation dynamics in the proposed model and to analyze its behavior. It was shown that propagation is favored by the initial position of the first infected device and the use of long-range antennas. In addition, the combination of the recovery and renewal processes in the smartphone population shows that infection can become endemic, if device density is medium or large.

This section analyzes user interaction. For this purpose, three different actions were reviewed: i) Activating the Bluetooth antenna; ii) Setting the device in discoverable mode; and iii) Accepting an incoming Bluetooth transmission. These three actions are modeled with changes in P_{BT}, P_D and P_{acc}, respectively.
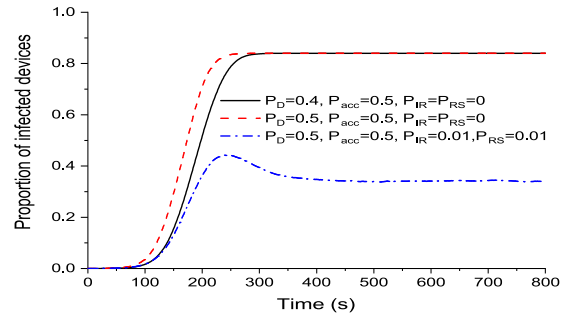
Thus, different specific scenarios for worm propagation can be designed which consider a smartphone user's level of cybersecurity awareness regarding the risks inherent in using these devices in Bluetooth networks. Examples could be, for instance, a scenario in which it is possible that a user decides to maintain the antenna on at all times, $P_{BT} = 1$, but in a dormant discoverable mode in order to be able to connect only with other previously paired devices, $P_D = 0$; or when a user maintains the antenna on, $P_{BT} = 1$, and activates the discoverable mode, $P_D = 1$, but the user accepts only some transfers, $0 < P_{acc} < 1$. Moreover, in addition to SL and RW movement patterns considered in previous simulations, this subsection also presents simulation results for the mixed movement with pauses (MMwP), defined in subsection II-F. The aim is to analyze malware propagation behavior when a more realistic human movement is taken into account. This movement pattern considers random pause times after an agent reaches one destination point before moving to a new one (see subsection II-F). This modification makes the MMwP more realistic than the SL and RW movements, because the model considers casual human behavior, since users typically pause for some time after reaching an intended destination.

For all simulations, one infected smartphone was placed at the center of the geographic space and $P_{r10} = 1$. Two density values of smartphones in the cellular space, high (0.9) and low (0.3), were considered.

Figs. 17 and 18 show simulation results for several value combinations of P_{IR}, P_{RS}, P_D, and P_{acc}. The last two probability values represent the user's level of cybersecurity awareness. Figs. 17a-17c correspond to low density, $\sigma = 0.3$, and Figs. 18a-18c correspond to high density, $\sigma = 0.9$. Both figures analyze the three different movement patterns, SL, RW, and MMwP. As can be observed in Figs. 17 and 18, simulation results indicate that even when recovery and renewal

(a) Straight Line, $\sigma = 0.3$.

(b) Random Walk, $\sigma = 0.3$.

(c) Mixed Movement with Pauses, $\sigma = 0.3$.
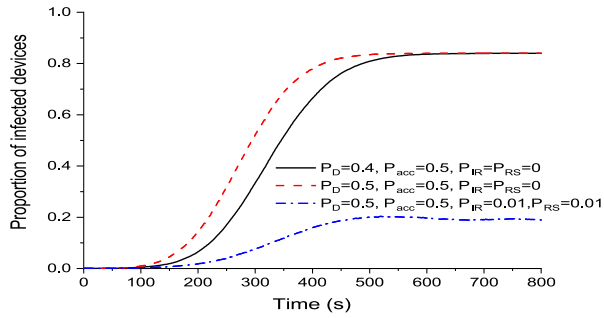
FIGURE 17. Effect of recover (P_{IR}) and renewal P_{RS}) probabilities on the time evolution of the infection for different values of P_{BT} and P_D, as well as different movement patterns with the outbreak starting at the center of the cell space and a population density $\sigma = 0.3$.
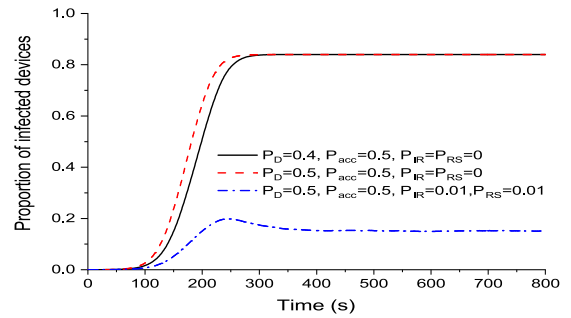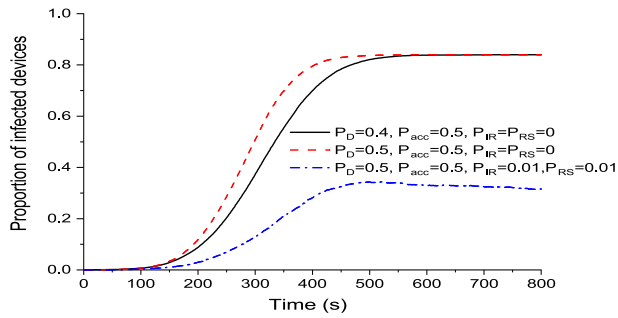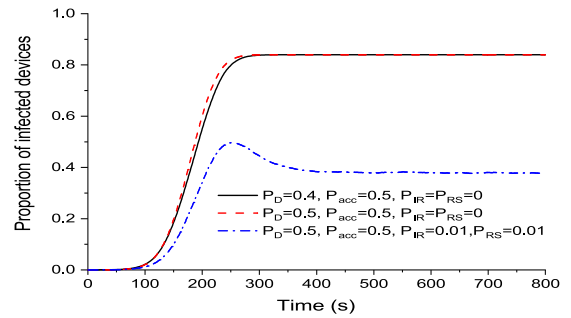

(a) Straight Line, $\sigma = 0.9$.
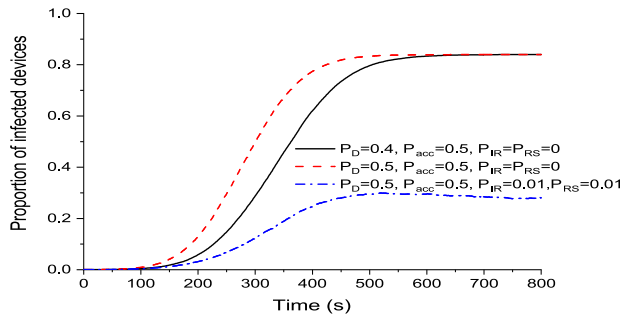
(b) Random Walk, $\sigma = 0.9$.

(c) Mixed Movement with Pauses, $\sigma = 0.9$.

FIGURE 18. Effects of recover (P_{IR}) and renewal (P_{RS}) probabilities on the time evolution of the infection for different values of P_D, P_{acc}, and different movement patterns with outbreak beginning in the center of the cell space C and population density $\sigma = 0.9$.

probabilities are not included, a better user cybersecurity awareness results in slower malware propagation, regardless of smartphone density. Besides, results also indicate that cybersecurity awareness, represented by the antenna's having the discoverable mode activated and the acceptance of incoming connections, plays a decisive role in worm expansion. This occurred even though the Bluetooth antenna was permanently on ($P_{BT} = 1$) during all simulations and even without a recovery mechanism. Moreover, results in Figs. 17 and 18 also indicate that when the recovery and renewal processes are taken into consideration, the worm is no longer able to affect the entire device population and its propagation capability is reduced, although without removing it completely from cell space C.

To analyze the effects of the different movement patterns on malware propagation, Fig. 19a shows the proportion of infected devices over time for SL, RW and MMwP movement patterns, for $P_D = P_{acc} = 0.5$, $P_{IR} = P_{RS} = 0.01$ and $\sigma = 0.3$ (low density), while Fig. 19b uses the same parameter values for $\sigma = 0.9$ (high density). In both cases, it was observed that the largest proportion of infected devices occurred with MMwP movement. This is a consequence of the pauses in the movement pattern that reduce transmission interruptions and favor malware infection and the possibility of moving in all directions, even in low-density environments. For SL and RW, malware propagation changes as a function of density. For low-density environments, a larger proportion of infection is achieved with RW movement; this is because users tend to
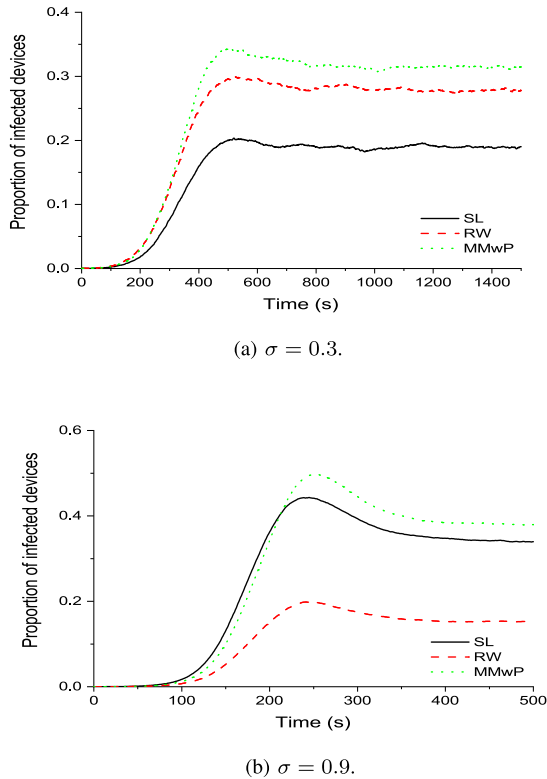
(a) $\sigma = 0.3$.

(b) $\sigma = 0.9$.

FIGURE 19. Time evolution of infected devices with different movement patterns for $P_D = P_{acc} = 0.5$, $P_{IR} = P_{RS} = 0.01$. Beginning of the outbreak in the center and population density $\sigma = 0.3$ and $\sigma = 0.9$.

move around in the same location and, considering that there are many available spaces to move to, malware propagation is favored. For high-density environments, a larger population of infected devices is achieved with SL movement, because smartphone users tend to move across larger routes than with the RW pattern, which is not favored by the reduced spaces existing between devices. These results confirm the importance of using realistic movement patterns for a more faithfully reproduction of the malware propagation behavior in cell space $\mathcal{C}$.

IV. CONCLUSION AND FUTURE WORK

Inspired by compartmental epidemiological models, this paper presented a new explicit spatio-temporal model to characterize worm propagation dynamics in smartphones using a two-dimensional cellular automaton. This model takes into account the individual characteristics of each device, such as security settings, latency time, and operating system type, among others. The simulations carried out implemented different motion patterns that allowed studying how the user's demographics affected the worm's propagation mechanics.

The paper analyzed different simulation scenarios that also considered user awareness about the risks inherent in using smart devices in Bluetooth networks. For this purpose, various probability values were obtained that describe the acceptance of incoming communication and the effects of recovery and immunity to threats by having some restoration

mechanism or by applying a backup. Besides, as smart device heterogeneity goes beyond the type of operating system, different types of antennas integrated into smart devices were also considered according to Bluetooth standard specifications, the transmission rate and range of which directly affect propagation speed. Based on all of these aspects, an analysis of propagation dynamics was carried out in order to determine how a Bluetooth worm might spread under specific scenarios.

Simulation results indicate that Bluetooth antenna range and rate are crucial factors to consider since they give an attacker more chances to reach a larger number of devices. Besides, the combination of the initial position of the infected smartphone and the type of motion also affected the outbreak over time. In particular, it was observed that the position at the center of the geographic space greatly favors worm propagation when limited spaces are considered. This could be important when an attacker propagates viruses or commits other cybercrimes in limited crowded areas. Furthermore, simulation results indicated that device density also has an impact on worm propagation. When density is low, spread speed is slow; as density increases, the worm spreads much faster since devices are close enough to each other to facilitate the spread of the worm. On the other hand, simulation results of two different motion patterns, random walk and straight line, indicate that a straight line pattern favors the worm's spreading in geographic spaces with low smartphone density.

Finally, when a more realistic movement pattern was simulated, mixed movement with pauses, the number of infected devices increased. However, user cybersecurity awareness can limit this increase.

In addition, when protection mechanisms are not considered, results indicated that the maximum number of infected smartphones was reached in a reduced time, a result that was expected. All these results together indicate, on the one hand, that crowded areas, implying a high density of devices, may be ideal for propagating worms to Bluetooth devices and, on the other hand, that positive user intervention is of key importance in limiting the effect of worm propagation.
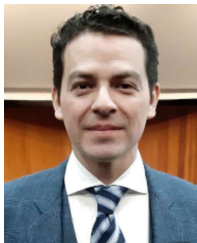
In future research, the model could analyze the effects of more realistic human motion patterns, such as origin-destination, and more detailed geographic areas, community models, or a combination of the two. The model could be extended beyond Bluetooth to include other transmission media.

REFERENCES

[1] Statista. *Number of Smartphone Users Worldwide 2014-2020*. Accessed: Sep. 20, 2020. [Online]. Available: https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/

[2] Ponemon Institute. (2018). *2018 Cost of a Data Breach Study: Global Interview*. [Online]. Available: https://databreachcalculator.mybluemix.net/assets/2018_Global_Cost_of_a_Data_Breach_Report.pdf

[3] BitDefender. (2010). *Malware History*. Accessed: Sep. 20, 2020. [Online]. Available: http://download.bitdefender.com/resources/files/Main/file/Malware_History.pdf

[4] H. Xiang, "Bluetooth-base Worm Modeling And Simulation," Ph.D. dissertation, Dept. Elect. Eng. Comput. Sci., Univ. Central Florida, Orlando, FL, USA, Jan. 2007. [Online]. Available: https://stars.library.ucf.edu/etd/3418 and http://purl.fcla.edu/fcla/etd/CFE0001740

[5] L. Chen, L. Feldman, and G. Witte, "Updated NIST guidance for Bluetooth security," Nat. Inst. Standards Technol., Tech. Rep. ITL Bull., Jul. 2017. [Online]. Available: https://csrc.nist.gov/CSRC/media/Publications/Shared/documents/itl-bulletin/itlbul2017-07.pdf

[6] (2003). *IEEE 802.15.4 WPANT Task Group 4 (TG4)*. Accessed: Sep. 20, 2020. [Online]. Available: http://www.ieee802.org/15/pub/TG1.html and http://www.ieee802.org/15/pub/TG4.html

[7] F-Secure Labs. *Bluetooth-Worm:SymbOS/Cabir Description | F-Secure Labs*. Accessed: Sep. 20, 2020. [Online]. Available: https://www.f-secure.com/v-descs/cabir.shtml

[8] F-Secure Labs. *Bluetooth-Worm:SymbOS/Commwarrior.B Description | F-Secure Labs*. Accessed: Sep. 20, 2020. [Online]. Available: https://www.f-secure.com/v-descs/bluetooth-worm_symbos_commwarrior_b.shtml

[9] Kaspersky. (2006). *Mobile Malware Evolution: An Overview, Part 1*. [Online]. Available: https://securelist.com/mobile-malware-evolution-an-overview-part-1/36109/

[10] Kaspersky. (2014). *Five Stories About Cabir, the First Malware for Smartphones*. [Online]. Available: https://www.kaspersky.com/blog/cabir-five-stories/14964/

[11] N. Husted and S. Myers, "Why mobile-to-mobile wireless malware won't cause a storm," in *Proc. 4th USENIX Workshop Large-Scale Exploits Emergent Threats, Botnets, Spyware, Worms, More*, 2011, pp. 1–7.

[12] Bluetooth SIG. (2018). *Bluetooth Market Update 2018*. Accessed: Sep. 22, 2020. [Online]. Available: https://bluetooth.com

[13] Armis Labs. (2017). *BlueBorne Information from the Research Team—Armis Labs*. Accessed: Sep. 20, 2020. [Online]. Available: https://armis.com/blueborne/

[14] B. Seri and G. Vishnepolsky, "The dangers of Bluetooth implementations: Unveiling zero day vulnerabilities and security flaws in modern Bluetooth stacks," in *Proc. ArmisLabs*, 2017, pp. 1–38. [Online]. Available: http://go.armis.com/hubfs/BlueBorneTechnicalWhitePaper-1.pdf?t=1508711403067

[15] A. Lonzetta, P. Cope, J. Campbell, B. Mohd, and T. Hayajneh, "Security vulnerabilities in Bluetooth technology as used in IoT," *J. Sensor Actuator Netw.*, vol. 7, no. 3, p. 28, Jul. 2018.

[16] P. H. O'Neill. (2020). *India is Forcing People to Use Its COVID App, Unlike Any Other Democracy*. [Online]. Available: https://www.technologyreview.com/2020/05/07/1001360/india-aarogya-setu-covid-app-mandatory/

[17] A. Illmer. (2021). *Singapore Reveals COVID Privacy Data Available to Police*. [Online]. Available: https://www.bbc.com/news/world-asia-55541001

[18] P. H. O'Neill, T. Ryan-Mosley, and B. Johnson. (2020). *A Flood of Coronavirus Apps are Tracking Us. Now It's Time to Keep Track of Them*. [Online]. Available: https://www.technologyreview.com/2020/05/07/1000961/launching-mittr-covid-tracing-tracker/

[19] European Commission. (2020). *How Tracing and Warning Apps Can Help During the Pandemic | European Commission*. [Online]. Available: https://ec.europa.eu/info/live-work-travel-eu/coronavirus-response/travel-during-coronavirus-pandemic/how-tracing-and-warning-apps-can-help-during-pandemic_en

[20] BBVA. (2020). *How do COVID-19 Tracing Apps Work and What Kind of Data do They Use?* [Online]. Available: https://www.bbva.com/en/how-do-covid-19-tracing-apps-work-and-what-kind-of-data-do-they-use/

[21] Health Canada. (2020). *Download COVID Alert: Canada's Exposure Notification App—Canada.ca*. [Online]. Available: https://www.canada.ca/en/public-health/services/diseases/coronavirus-disease-covid-19/covid-alert.html

[22] New Zealand Government. (2020). *NZ COVID Tracer App | Unite Against COVID-19*. [Online]. Available: https://covid19.govt.nz/health-and-wellbeing/protect-yourself-and-others/keep-track-of-where-youve-been/nz-covid-tracer-app/

[23] R. Pegoraro. (2020). *Google and Apple-Supported Coronavirus Tracking Apps Land From States*. [Online]. Available: https://www.usatoday.com/story/tech/columnist/2020/08/25/google-and-apple-supported-coronavirus-tracking-apps-land-states/3435214001/

[24] X. Xiao, P. Fu, C. Dou, Q. Li, G. Hu, and S. Xia, "Design and analysis of SEIQR worm propagation model in mobile Internet," *Commun. Nonlinear Sci. Numer. Simul.*, vol. 43, pp. 341–350, Feb. 2017.

[25] W. O. Kermack and A. G. McKendrick, "A contribution to the mathematical theory of epidemics," *Proc. R. Soc. Lond. A, Math. Phys. Sci.*, vol. 115, no. 772, pp. 700–721, 1927. [Online]. Available: http://rspa.royalsocietypublishing.org/cgi/doi/10.1098/rspa.1927.0118

[26] J. W. Mickens and B. D. Noble, "Modeling epidemic spreading in mobile environments," in *Proc. 4th ACM Workshop Wireless Secur. (WiSe)*. New York, NY, USA: ACM, 2005, p. 77. [Online]. Available: http://portal.acm.org/citation.cfm?doid=1080793.1080806

[27] K. Ramachandran and B. Sikdar, "On the stability of the malware free equilibrium in cell phones networks with spatial dynamics," in *Proc. IEEE Int. Conf. Commun.*, Jun. 2007, pp. 6169–6174. [Online]. Available: http://ieeexplore.ieee.org/document/4289692/

[28] K. Ramachandran and B. Sikdar, "Modeling malware propagation in networks of smart cell phones with spatial dynamics," in *Proc. IEEE INFOCOM-26th IEEE Int. Conf. Comput. Commun.*, Jul. 2007, pp. 2516–2520. [Online]. Available: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=4215894

[29] C. J. Rhodes and M. Nekovee, "The opportunistic transmission of wireless worms between mobile devices," *Phys. A, Stat. Mech. Appl.*, vol. 387, no. 27, pp. 6837–6844, Feb. 2008. [Online]. Available: http://arxiv.org/abs/0802.2685, doi: 10.1016/j.physa.2008.09.017.

[30] J. Sathyan, N. Anoop, N. Narayan, and S. K. Vallathai, *A Comprehensive Guide to Enterprise Mobility*. Boca Raton, FL, USA: CRC Press, 2016.

[31] W. Xia, Z.-H. Li, Z.-Q. Chen, and Z.-Z. Yuan, "Commwarrior worm propagation model for smart phone networks," *J. China Universities Posts Telecommun.*, vol. 15, no. 2, pp. 60–66, Jun. 2008. [Online]. Available: https://www.sciencedirect.com/science/article/abs/pii/S100588850860085 0

[32] S.-M. Cheng, W. C. Ao, P.-Y. Chen, and K.-C. Chen, "On modeling malware propagation in generalized social networks," *IEEE Commun. Lett.*, vol. 15, no. 1, pp. 25–27, Jan. 2011. [Online]. Available: http://ieeexplore.ieee.org/document/5638768/

[33] J. T. Jackson and S. Creese, "Virus propagation in heterogeneous Bluetooth networks with human behaviors," *IEEE Trans. Dependable Secure Comput.*, vol. 9, no. 6, pp. 930–943, Nov. 2012. [Online]. Available: http://ieeexplore.ieee.org/document/6268271/

[34] S. Peng, G. Wang, and S. Yu, "Modeling the dynamics of worm propagation using two-dimensional cellular automata in smartphones," *J. Comput. Syst. Sci.*, vol. 79, no. 5, pp. 586–595, Aug. 2013. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0022000012001754

[35] Z. Bakhshi, M. Z. Lighvan, and R. Mostafavi, "MP-CA: A malware propagation modeling methodology based on cellular automata," *Int. J. Comput. Netw. Commun. Secur.*, vol. 3, no. 3, pp. 63–73, 2015.

[36] Y. Hu, "Cellular automata model to simulate the spreading of mobile phone messages virus," *J. Inf. Comput. Sci.*, vol. 10, no. 11, pp. 3579–3586, Jul. 2013. [Online]. Available: http://www.joics.com/publishedpapers/2013_10_11_3579_3586.pdf

[37] Y. Song and G.-P. Jiang, "Modeling malware propagation in wireless sensor networks using cellular automata," in *Proc. Int. Conf. Neural Netw. Signal Process.*, Zhenjiang, China, Jun. 2008, pp. 623–627.

[38] S. Peng and G. Wang, "Worm propagation modeling using 2D cellular automata in Bluetooth networks," in *Proc. IEEE 10th Int. Conf. Trust, Secur. Privacy Comput. Commun.*, Nov. 2011, pp. 282–287.

[39] Á. M. del Rey and G. R. Sánchez, "A CA model for mobile malwarespreading based on Bluetooth connections," in *Proc. Int. Joint Conf. SOCO-CISIS-ICEUTE*, 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. Springer, 2014, pp. 619–629.

[40] 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 *Bioinspired Computation in Artificial Systems* (Lecture Notes in Computer Science: Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), vol. 9108. Cham, Switzerland: Springer, 2015, pp. 107–116. [Online]. Available: http://link.springer.com/10.1007/978-3-319-18833-1_12

[41] S. Wolfram, *Cellular Automata and Complexity*, vol. 1. Reading, MA, USA: Addison-Wesley Pub. Co, 2002.

[42] G. G. Garcia and M. E. L. Ramirez, "Modeling the spatio-temporal dynamics of worm propagation in smartphones based on cellular automata," in *Proc. Eur. Model. Symp. (EMS)*, Nov. 2016, pp. 196–201.

[43] G. G. García, M. E. L. Ramírez, and L. Alvarez-Icaza, "Worm propagation modeling considering smartphones heterogeneity and people mobility," in *Proc. Int. Conf. Appl. Math., Modeling Simulation (AMMS)*, vol. 153. Shanghai, China: Atlantis Press, Nov. 2017, pp. 147–152. [Online]. Available: http://www.atlantis-press.com/php/paper-details.php?id=25887979

[44] J. Padgette, J. Bahr, M. Batra, M. Holtmann, R. Smithbey, L. Chen, and K. Scarfone, "NIST special publication 800-121 revision 2 guideto Bluetooth security," Nat. Inst. Standards Technol., Tech. Rep. ST SP 800-121 Rev.2, 2017. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-121r2.pdf

[45] G. Yan and S. Eidenbenz, "Bluetooth worms: Models, dynamics, and defense implications," in *Proc. 22nd Annu. Comput. Secur. Appl. Conf. (ACSAC)*, Dec. 2006, pp. 245–256. [Online]. Available: http://ieeexplore.ieee.org/document/4041171/

[46] U. Khan. (2009). *12 Million People Suffered a Computer Virus Attack in the Last Six Months—Telegraph*. Accessed: Sep. 25, 2020. [Online]. Available: https://www.telegraph.co.uk/technology/news/5317908/12-million-people-suffered-a-computer-virus-attack-in-the-last-six-months.html

[47] H. Pilz and M. Morgenstern, "Useful and useless statistics about viruses and anti-virus programs," Helsinki, Finland, 2010, p. 10. [Online]. Available: https://archive.f-secure.com/weblog/archives/Maik_Morgenstern_Statistics.pdf

[48] R. Poston. (2010). *How Large is a Piece of Malware?—Naked Security*. Accessed: Sep. 21, 2020. [Online]. Available: https://nakedsecurity.sophos.com/2010/07/27/large-piece-malware/

[49] T. Marques. (2016). *PNG Embedded—Malicious Payload Hidden in a PNG File*. Accessed: Sep. 22, 2020. [Online]. Available: https://securelist.com/png-embedded-malicious-payload-hidden-in-a-png-file/74297/

MARÍA ELENA LÁRRAGA received the B.S. degree in computer sicience from the Benenérita Universidad Autónoma de Puebla, Mexico, and the master's degree in computer science and engineering and the Ph.D. degree in system engineering (Transport) from the Universidad Nacional Autónoma de México. She is currently working as a Researcher with the Universidad Nacional Autónoma de México. Her research interest includes modeling and simulation of complex systems such as, traffic flow analysis, epidemics, security, and malware propagation.

LUIS ALVAREZ-ICAZA (Member, IEEE) received the B.S. degree in mechanical engineering and the master's degree in electrical engineering with major in automatic control from the Universidad Nacional Autónoma de México (UNAM), and the Ph.D. degree in mechanical from Berkeley California. He is currently working as a Researcher with the Universidad Nacional Autónoma de México. Moreover, he is a National Researcher (SNI). His research interests include control theory and modeling and identification of electro-mechanical.

GABRIEL GONZÁLEZ received the M.S. degree in computer science and engineering from the Universidad Nacional Autónoma de México (UNAM), in 2017. He is currently pursuing the Ph.D. degree in computer science and engineering. His research interests include software engineering, malware propagation, and modeling and simulation of complex systems. He was awarded with the Alfonso Caso Medal 2017 by UNAM, for academic achievements.

JAVIER GOMEZ received the B.Tech. degree in electrical engineering from the School of Engineering, Universidad Nacional Autónoma de México (UNAM), and the master's and Ph.D. degrees in electrical engineering from Columbia University. He is currently a Research-Professor in telecommunications networks with the School of Engineering, UNAM. His research interests include performance modeling, analysis and design of algorithms, protocols for wireless ad hoc, and sensor and mesh networks.

• • •