ATLANTIS PRESS

Advances in Intelligent Systems Research, volume 153

International Conference on Applied Mathematics, Modeling and Simulation (AMMS 2017)

Worm Propagation Modeling Considering Smartphones Heterogeneity and People Mobility

Gabriel González García, María Elena Lárraga Ramírez* and Luis Alvarez-Icaza

Instituto de Ingeniería, Universidad Nacional Autónoma de México, 04510, Coyoacán, México, D.F.

*Corresponding author

***Abstract*—In recent years, the worldwide market for smartphones has grown dramatically. The kind of information stored in these devices makes them an attractive target for malware writers. Consequently, modeling of worm propagation in smartphones in order to predict the side effects of a new threat and understand the complex behavior of the modeled malware has received significant attention. One of the possible mechanisms for malware spreading are Bluetooth antennas, where the malware infects devices in its proximity as biological viruses do. Due to this strong similarity in the behaviors of self-replicating and propagation between mobile malware and biological viruses, most investigations of malware propagation in smartphones focus predominately on modeling its propagation dynamics by employing the classical epidemic theories in epidemiology. Cellular Automata (CA) models have emerged recently as a promising alternative to characterize worm propagation and understand its behavior. However, in the most of the existing CA models for mobile malware, it is assumed that all smartphones are homogeneous and that transmission time of the worm is one time cycle. In this work, a mathematical model to study the spatio-temporal propagation dynamics of Bluetooth worms based on CA and the compartmental epidemiological models is introduced. The model considers the local interactions between the smartphones and is able to simulate the individual dynamic of each device and the effect of mobility of their users on the infection propagation.**

Keywords-component; cellular automata; complex systems modelling; bluetooth networks

I. INTRODUCTION

The market and use of mobile telephony has grown rapidly, according to Statista, in 2017 the number of mobile phone users is forecast to reach 2.32 billion [1]. Smartphones enable users to download individual programs that can perform a variety of tasks, however, the availability of these mobile services provided by smartphones increases their vulnerability to malware attacks. Of particular interest is the malware which is propagated using Bluetooth connections, since it infects devices in its proximity as biological viruses do. It is precisely because of the strong similarity in the behaviors of self-replicating and propagation between mobile malware and biological viruses, that most investigations of malware propagation in smartphones focus predominately on modeling the malware propagation by employing the classical epidemic theories in epidemiology [2]. Consequently, modeling of worm propagation in smartphones in order to predict the side effects of a new threat and understand the behavior of the modeled malware has received significant attention in recent years [3,4]. Unfortunately, not many mathematical models dealing with the prediction of the behavior of the spreading of mobile malware exist, and this number is even smaller if they are related to Bluetooth malware. Most of these works are based on continuous mathematical tools such as systems of ordinary differential equations (see [5-12]). These type of models does not take into account local interactions between the smartphones, assume that the elements forming the network are distributed homogeneously and that all are connected with one another, and therefore, they are unable to simulate the individual dynamic of each of the smartphones of the network.

In order to model spatial-temporal spreading, Cellular Automata (CA) models have emerged recently, as a promising alternative to characterize worm propagation and understand its behavior [13-20]. CA are dynamical systems, which operate in finite and discrete space and time [21] and whose dynamics is based on local rules that allow to capture micro-level dynamics and to propagate them to macro-level. Peng et.al. [13-17] proposed a CA model whose dynamics is based on infected resistence factors and no other characteristics are considered. On the other hand, in the model by Martín et. al [19], different types of operating system and the mobility of the smartphones are considered, however, the approach still has some limitations such as the scenario where worm propagation is interrupted by the smartphone mobility, e.g. the smartphone moves away from the antenna of the infected smartphone breaking infection dynamic.

In [22] authors proposed a discrete mathematical model to simulate Bluetooth- based worn spreading on smartphones by using CA. Specifically, the propagation of a worm is studied by means of a model where seven classes of epidemic states for a smartphone are considered: susceptible, exposed, carrier, infected, diagnosed, recovered, and interrupted. Based on these epidemic states, a set of local rules is designed to model the propagation dynamics when heterogeneous smartphones and their mobility in the area under study are considered. However, results with heterogeneous devices were not presented in this work and the number of infected devices on time is underestimated.

The main goal of this work is to improve the work [22] to represent in a better way malware spreading on time and space. For this purpose, the state diagram that defines the dynamics of the model is changed to work more properly, in particular, when heterogeneous smartphones with different operating systems and the influence of the mobility on the spreading of the malware are considered. Moreover, it will be assumed in

the new model that security countermeasures (antivirus software) are efficient against worms, that is, reinfection process is not allowed. Simulation results indicate that the proposed model allows to capture the dynamics of Bluetooth worm propagation and facilitates predictions of the evolution of the malware spreading in time and space of the individual devices. In addition, the computational cost of the model is low.

The rest of this paper is organized as follows. In Section 2, the proposed model is presented. Some illustrative simulation results are presented in Section 3. Finally, the conclusions and future work are introduced in Section 4.

II. THE MODEL

The model consists of a single layer probabilistic CA that is composed of N smartphones which are randomly arranged on a 2-D array of $M \times M$ cells (the cellular space). Each cell may be empty or occupied by just one smartphone at each time-step, the model increases the time in discrete time-steps such as $t \rightarrow t + 1$. In consequence, state variables change over time according to the transition state diagram shown in Figure I. Thus, the cellular space, denoted as C, represents the geographical space occupied by devices under study. To simplify the investigation, we assume that the horizontal and vertical coordinates of a smartphone are represented by i and j in the cellular space. In addition, the neighborhood of each cell is defined according to the corresponding transmission range r of the Bluetooth antenna. It is important to say that both, the radius r and the population of smartphones N will remain constant during the execution of all simulations.

A. States of Smartphones

According to the propagation property of Bluetooth worms, the state of a smartphone at time-step t is divided in six compartments in such a way that for a smartphone u located in a cell on the position (i,j) at time t, its state is represented as $\omega_{i,j}^{t}$, and belongs to the set of values {S, E, C, I, R, INT} which are defined as follows:

1) Susceptible state (S). Healthy devices which are vulnerable to the worm if they move into the Bluetooth antenna transmission range of an infected device.

2) Exposed state (E). Susceptible devices that are connected to an infected device, which is sending a copy of the worm. Exposed devices are unable to start contagions until they have the full worm payload.

3) Carrier state (C). Devices who have received a full copy of a specific worm, but their operating system does not match the operating system for which it was designed, preventing the worm coming into operation and consequently, preventing it from spreading. This state is a terminal state.

4) Infected state (I). Devices with a fully functional copy of the worm which is in operation. Infected devices can infect other susceptible devices found in their neighborhood (transmission range).

5) Recovered state (R). Devices to which the worm has been removed permanently after identifying the menace, giving them immunity from further contagion of the same malware due to the installation of an antivirus software. This state is a terminal state.

6) Interrupted state (INT). Exposed devices which were connected to an infected smartphone and they moved away from the Bluetooth antenna reach of the infected smartphone. These devices will go back to susceptible state at time $t + 1$.

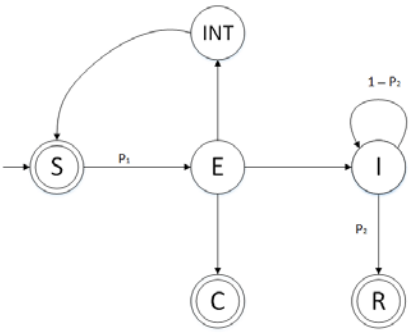

FIGURE I.STATE TRANSITION RELATIONSHIP FOR BLUETOOTH WORM PROPAGATION

The process of state change for worm propagation is illustrated in Figure. I. Here, P_1 is the probability with which a smartphone in state S transitions to state E and P_2 denotes the probability with which a smartphone in state I transitions to state R, otherwise it will remain in state I.

On the other hand, the Bluetooth antenna range will be modeled by using a Moore neighborhood [23], where r will stand for the range of transmission of antenna. In such a way that according to the corresponding transmission range r, the neighborhood of each cell is defined. A Moore neighborhood is composed of a central cell and the $(2r + 1)^2$ cells which surround it. Thus, the number of neighbors of the node increases as a function of r. Therefore, the neighborhood represents the area to establish connections in a network of devices with Bluetooth antennas, which are made on the fly between devices that are within the range of another devices that is willing to start a transmission.

B. Smartphone Attributes

Each smartphone deployed in the lattice is represented by an agent which is used for abstracting relevant features of these devices. The attributes considered in Table I allow to model local interactions between connected smartphones and how they affect propagation dynamics of the worm.

Once the smartphones are deployed throughout geographical area C, they can move randomly with a probability P_{Mov}. During each time-step, a smartphone can move from its current position to a neighbor cell if and only if the destination cell is available and P_{Mov} is met. The selected direction of movement for a given smartphone is determined from a set of values which represents the cardinal points north, south, east, west, northeast, northwest, southeast, and southwest, in a random way. If a movement is not possible, the smartphone will remain at its position during time-step t and

then, a new movement direction will be recalculated using the same criteria explained before, at time *t + 1*.

C. Transition between States

Each smartphone will evolve on each time-step according to the following rules, which depends on the current state of the cell under evaluation:

Susceptible to exposed state. Let us suppose that the smartphone of interest is in the cell *u*, whose current state is susceptible (S), this will change to state exposed (E) if any of its neighbors *v* meet probability P_1 defined as follows:

$$P_1 = \beta \frac{I_u(t)}{N_u(t)} \tag{1}$$

where N_u is the total number of neighbors of cell *u*. The model assumes that an infected smartphone will always have its Bluetooth antenna on, therefore, to determine whether the connection between a susceptible smartphone is established with an infected smartphone, two conditions must be met: the susceptible device that is being contacted has its Bluetooth antenna turned on and it accepts the incoming connection. A logic function used to model the condition that determines whether a contact between the cell *u* and the cell *v* is established is given by

$$FL_1 = u_{BT} \wedge u_{accept\_conn\_v} \tag{2}$$

where u_{BT} represents a logical value, where 1 indicates that the antenna of the cell *u* is turned on according with the probability ε or it is turned off with probability 1– ε.

$u_{accept\_conn\_v}$ also takes a logical value, where a value equal to 1 indicates that the smartphone located in the cell *u* accepts the incoming connection from cell *v*, with a probability α or it is rejected with a probability 1 – α.

Thus, the transition of state of the smartphone in cell *u* from a susceptible state to state exposed is defined as follows:

$$\text{if } ((Rand() \leq P_1) \wedge FL_1 = 1) \tag{3a}$$

$$\omega_{i,j}^{u}(t+1) \rightarrow E$$

$$\text{if } \neg((Rand() \leq P_1) \wedge FL_1 = 1) \tag{3b}$$

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

where Rand() ∈ [0, 1] and denotes a uniform random number, denotes the logical operator NOT, and ∧ denotes logical operation AND.

Exposed to infected or exposed to interrupted or exposed to carrier state. Let *u* denoting the location of a smartphone whose current state is exposed (E). This will change to an interrupted (INT), an infected (I), or a carrier (C) state according to the following logic functions:

$$\text{if } (t < (IST + T)) \tag{4a}$$

$$\text{if } (v_{infected} \in V_u)$$

$$\omega_{i,j}^{u}(t+1) \rightarrow E$$

$$\text{if } (v_{infected} \notin V_u)$$

$$\omega_{i,j}^{u}(t+1) \rightarrow INT$$

$$\text{if } (t \geq (IST + T)) \tag{4b}$$

$$\text{if } (v_{infected} \in V_u \wedge u_{OS} = v_{OS})$$

$$\omega_{i,j}^{u}(t+1) \rightarrow I$$

$$\text{if } (v_{infected} \in V_u \wedge u_{OS} \neq v_{OS})$$

$$\omega_{i,j}^{u}(t+1) \rightarrow C$$

where *t* represents the current time-step, V_u represents the neighborhood of *u*, and u_{os} and v_{os} represent the operative system of *u* and *v*, respectively. As shown in Eq. (4b), once the latency time *T* is over, the next state will be decided by the type of operating system of the smartphones. In particular, an infected smartphone must stay in the range of transmission to reach an exposed smartphone *u*, during all latency time *T* required to transmit the full worm payload. This calculation will be counted individually, supported by the *infection start time attribute* (IST) of each agent representing the exposed device, so that the time displacement obtained by *IST* + *T* will result in the time-step when *u* will pass to infected state.

Interrupted to susceptible state. Let *u* denoting the location of a smartphone, whose current state is interrupted (INT), this will go back to susceptible (S) state unconditionally at next time-step. This represents the fact that the connection between an infected and an exposed smartphone was broken, but the exposed smartphone is vulnerable to be contacted once again by another infected device.

$$\omega_{i,j}^{u}(t+1) \rightarrow S \tag{5}$$

Infected to recovered state. Let *u* denoting the location of a smartphone, whose current state is infected (I). This will change its sate to recovered (R) state if probability P_2 is met. Otherwise, it will remain in infected (I) state indicating that the attempt to detect and remove the worm failed. This probability is calculated as follows:

$$\text{if } (Rand() \leq P_2) \tag{6a}$$

$$\omega_{i,j}^{u}(t+1) \rightarrow R$$

$$\text{if } (Rand() > P_2) \tag{6b}$$

$$\omega_{i,j}^{u}(t+1) \rightarrow I$$

Graphically, the state transitions described before are shown in Figure. I.

D. General Considerations of the Model

- This model considers only as an infection vector the Bluetooth connections.
- Smartphones may have different operating configuration and security systems affecting the spread of the worm.
- The dynamics of infection is from an infected smartphone to another "healthy" one. To consider that an infection is successful, the healthy device must be in the transmission range of smartphone infected throughout the time required for transmission of the worm (time latency).
- An exposed smartphone can be connected only with one infected smartphone at time *t* and vice versa.
- A smartphone that has been infected and recovered subsequently acquires final worm immunity. If there is any connection with an exposed smartphone, it will be canceled by passing the state INT.
- Only susceptible smartphones can be infected.
- Smartphones in the state INT will pass to susceptible state at time *t + 1*.
- The model evolves in time-steps *t* equal to 1 second.

III. SIMULATIONS AND RESULTS

In this section, simulation results from the proposed model are presented. A geographical area of 101 × 101 cells, with a cell length of 1 m. is considered for all presented simulations results, which can represent a block in a residential area. The input parameters of the model are shown in Table I. For each simulation result presented (except for the spatio-temporal diagram) 10 simulation runs are made and the obtained results are then averaged.

The population density of smartphones σ is calculated by (7), where *N* represents the number of smartphones deployed in the two-dimensional cellular space *C*.

$$\sigma = \frac{N}{C} \tag{7}$$

The susceptible device is maintained in the range of the Bluetooth antenna of an infected device throughout the latency time required until malware is transmitted completely. To model this event, the state of interrupted (INT) comprises all those exposed devices that go out of transmission range of infected smartphone before completing the transmission of the worm, then devices in this state will return to susceptible state again at next time-step. All tests consider a heterogeneous population of smartphones (Android, iOS and Windows operating systems).

All tests start from $P_2 = 0$ to $P_2 = 0.05$ with increments of 0.01, and $P_{Mov} = 0.1$, whereas the probability that Bluetooth antenna is turned on ε and the probability of acceptance of the connection α are assigned to 1 and the density of smartphones values considered are 60%, 70%, 80% and 90%. For each simulation, the stop condition is either when the maximum time is reached or the 95% of total density of smartphones is infected by the worm.

In Figure II the evolution of the infectious smartphones of the system is shown when different operative systems are considered, the number of infectious devices at initial step of time is equal to 10%, $P_{Mov} = 0.1$ and $P_2 = 0$, which represents that smartphones have no mechanism of defense against the worm. Note that, independently of the density, the trends are similar: in all cases a quasi-endemic equilibrium is reached.

TABLE I. PARAMETERS AND VARIABLES

Simulation duration	21,600 ticks (6 hours)
Cellular space size	101 × 101 m2
Number of simulations	10
Infection rate β	0.9
Latency time T	25 seconds
Type of neighborhood	Moore
CA boundary	Assigned
Density of initial infected I(0)	10%
Bluetooth antenna range r	1 m

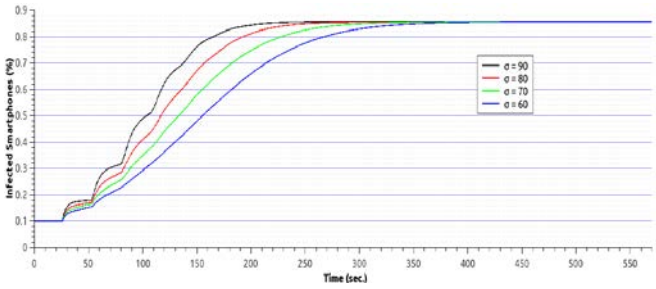

FIGURE II. INFECTED SMARTPHONES WITH $P_2=0$ AND $P_{MOV}=0.1$ ACCORDING TO DENSITY σ

However, as soon as the probability of removal $P_2 \geq 0$, the propagation dynamics of the worm is highly affected as it is show in figures III and IV, for P_2=0.01 and P_2=0.03, respectively: The larger P_2 is, the faster the infection decreases.

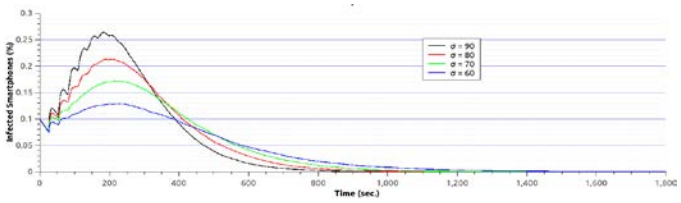

FIGURE III. THE EVOLUTION OF THE INFECTIOUS SMARTPHONES FOR P_2=*0.01* AND P_{MOV}=*0.1* AND DIFFERENT DENSITY VALUES, σ.

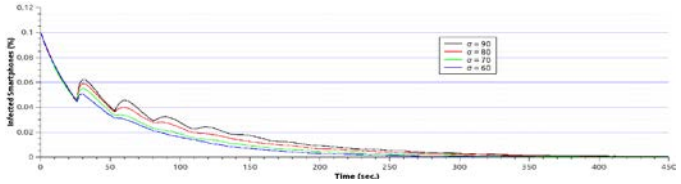

FIGURE IV. THE EVOLUTION OF THE INFECTIOUS SMARTPHONES FOR P_2=*0.03* AND P_{MOV}=*0.1* AND DIFFERENT DENSITY VALUES, σ.

Finally, in Figure V the spatio-temporal evolution of infection at different time-steps for P_{Mov} = 0.1 and P_2=0.03 is shown, where it can be observed that the infection point is reached near to *t = 300*. White dots denote susceptible devices, yellow dots denote exposed devices, and red dots denote infectious devices.

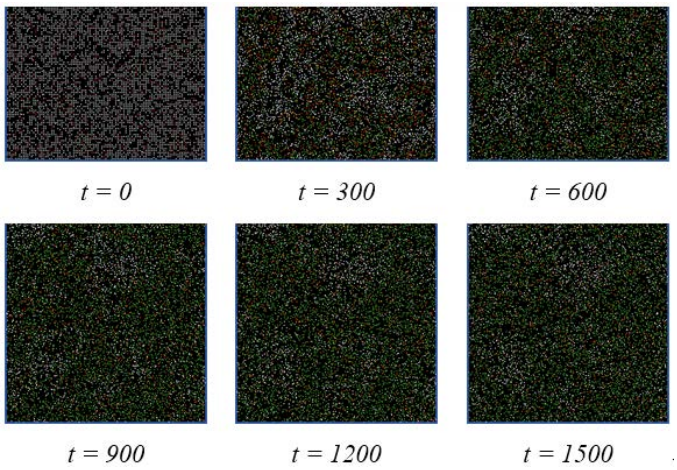

FIGURE V. SPATIAL-TEMPORAL DIAGRAM OF THE FIRST 1500 TIME-STEPS

IV. CONCLUSIONS

In this work, a new spatio-temporal model to characterize the dynamics of worm propagation in smartphones using a two-dimensional cellular automata was presented. The model introduces a suitable set of rules that takes into account the interruption of the worm propagation due to the movement of the smartphones. Six classes of epidemic states for a smartphone were considered: susceptible, exposed, carrier, infected, recovered, and interrupted. The transmission vector is given by the Bluetooth connections. Simulation results indicate that the proposed model allows to capture the dynamics of Bluetooth worm propagation and facilitates predictions of the evolution of the malware spreading in time and space of the individual devices. In addition, the computational cost of the model is low, making it suitable to predict the spreading curves of Bluetooth worm propagation in large areas.

As a future work, we will focus on analyzing the propagating characteristics of hybrid viruses such as e-mail, MMS and SMS.

ACKNOWLEDGMENT

This work was supported by DGAPA-UNAM under project IN112716 and CONACyT (Grant No. 156667).

REFERENCES

[1] Statista, "Number of smartphone users worldwide 2014-2020 | Statista," [Online]. Available: https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/. [Accessed 18 September 2017].

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

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

[4] del Rey, A. M. "Mathematical modeling of the propagation of malware: a review". Security Comm. Networks, 8: 2561–2579, January 2015, doi: 10.1002/sec.1186.

[5] Cheng, S.M., Ao, W.C., Chen, P.Y., Chen, K.C.: On Modeling Malware Propaga-tion in Generalized Social Networks. IEEE Commun. Lett. 15(1), 25–27 (2011)

[6] Jackson, J.T., Creese, S.: Virus Propagation in Heterogeneous Bluetooth Networks with Human Behaviors. IEEE T. Depend. Secure 9(6), 930–943 (2012)

[7] Mickens, J.W., Noble, B.D.: Modeling Epidemic Spreading in Mobile Environments. In: Proc. of the 4th ACM Workshop on Wireless Security, pp. 77–86. ACM Press, NY (2005)

[8] Ramachandran, K., Sikdar, B.: On the Stability of the Malware Free Equilibrium in Cell Phones Networks with Spatial Dynamics. In: Proc. of the 2007 IEEE International Conference on Communications, pp. 6169–6174. IEEE Press (2007)

[9] Ramachandran, K., Sikdar, B.: Modeling Malware Propagation in Networks of Smart Cell Phones with Spatial Dynamics. In: Proc. of the 26th IEEE International Conference on Computer Communications, pp. 2516–2520. IEEE Press (2007)

[10] Rhodes, C.J., Nekovee, M.: The opportunistic transmission of wireless worms between mobile devices. Physica A 387, 6837–6844 (2008)

[11] Sathyan, J., Anoop, N., Narayan, N., Vallathai, S.K.: A Comprohensive Guide to Enterprise Mobility. CRC Press (2012)

[12] Wei, X., Zhao-Hui, L., Zeng-Qiang, C., Zhu-Zhi, Y.: Commwarrior worm propagation model for smart phone networks. J. China U Posts Telecommun. 15(2), 60–66 (2008)

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

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

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

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

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

[18] S. Peng, G. Wang, S. Yu, “Modeling the dynamics of worm propagation using two-dimensional cellular automata in smartphones”, Journal of Computer and System Sciences, Volume 79, Issue 5, 586-595, August 2013, doi:10.1016/j.jcss.2012.11.007.

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

[20] Á. Martín del Rey, G. Rodriguez-Sanchez, “A Cellular Automata Model for Mobile Worm Propagation”, Bioinspired Computation in Artificial Systems: International Work-Conference on the Interplay Between Natural and Artificial Computation, IWINAC 2015, Elche, Spain, June 1-5, 2015, Proceedings, Part II

[21] S. Wolfram, «Wolfram on Cellular Automata and Complexity,» Los Alamos Science, vol. 9, pp. 2-21, 198.

[22] Gabriel Gonzalez Garcia, María E. Lárraga Ramírez, Modeling the Spatio-Temporal Dynamics of Worm Propagation in Smartphones Based on Cellular Automata. EMS 2016: 196-201.

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