Advanced malware propagation on random complex networks

A. Martín del Rey[a,*], G. Hernández[b], A. Bustos Tabernero[a], A. Queiruga Dios[a]

[a] *University of Salamanca, Institute of Fundamental Physics and Mathematics Department of Applied Mathematics, Salamanca, Spain*
[b] *University of Salamanca, BISITE Reasearch group, Salamanca, Spain*

Abstract

In this work a novel model to simulate advanced malware spreading is introduced and analyzed. It is an individual-based model such that the dynamics of the malware outbreak is governed by means of a cellular automaton. The network topologies considered are complex random networks and each device is endowed at every step of time with one of the following possible states: susceptible, infected, attacked and recovered. A study analyzing the influence of topology variability and the structural characteristics of initially infected devices is done.

Keywords: Malware propagation, random complex networks, individual-based model, cellular automata, advanced persistent threats (APTs).

1. Introduction

Advanced persistent threats (APTs for short) can be defined as highly specialized long-term cyber-attacks which are perpetrated by well-trained, well-funded organized teams with great technological and computational resources and abilities [1, 2]. These special cyber-attacks are usually sponsored by government agencies or criminal organizations with large amount of resources of

*This is an extended and improved version of the work entitled "Modeling the spread of malware on complex networks" presented at DCAI 2019 conference.

*Corresponding author
Email address: delrey@usal.es (A. Martín del Rey)

all kinds [3]. Several advanced logical tools are involved in this type of cyber-threats and, probably, the most important is the use of advanced malware that exploits zero-day vulnerabilities. Advanced malware is characterized by implementing evasive or stealthy techniques with the aim to attack predetermined and specific targets.

Consequently, it is very important to study the processes that rule the propagation of this malware specimen. These analysis allows us not only make predictions about the behavior of advanced malware spread but it is also possible to test the effectiveness of control procedures or security countermeasures. This conceptual framework is specified in the theoretical design and computational development of mathematical models for malware propagation (see, for example, [4, 5, 6]).

Since 1989, when the first mathematical model to simulate computer virus spread appeared [7], several different models have been proposed (see, for example, [8, 9, 10, 11] and references therein). The great majority are global or networked models with compartments defined by devices with the same topological characteristic –the number of contact neighbors– and endowed with the same state –susceptible, infected, recovered, etc.– (see, for example [12, 13, 14, 15]). All these models are devoted to the study of "classical" malware specimens (computer viruses, computer worms, etc.) and very few are related to the study of the propagation of advanced malware (see [16, 17, 18]). These models have limited practical applications since they do not take into account neither local interactions between devices nor individual characteristics of each device. To overcome these drawbacks the individual-based paradigm (IB-models) has been adopted in the last years considering both Agent-based models (ABM for short) and cellular automata models [19, 20], such that in this new approach each device/individual is represented as a set of characteristics that change dynamically over time. Taking into account this paradigm, some (not many) models have been proposed in the scientific literature. For example, in [21] an analytical model and its ABM version are proposed to simulate malware propagation over scale-free networks; in [22] the authors introduce an open-source and

flexible ABM considering local network structure, user mobility and application-level interactions, and malware network coordination; in [23] an epidemiological model based on a two-dimensional cellular automata is described considering a multi-player evolutionary game to predict the spread of a malware specimen in a wireless sensor network; in [24] a new model for malware propagation in complex networks using cellular automata is proposed where the nodes/devices are endowed with different anti-attack abilities; also the use of one-dimensional cellular automata has been considered for malware simulation purposes as is shown in [25]. In [26] the authors propose an individual-based model where each device –that stands for a node of a complex network– can be susceptible or infected at each step of time. Then it is a SIS compartmental model; moreover it is a stochastic model considering two purely epidemiological coefficients: the infection and curing rate. In [27] a general work defining an ABM framework to represent mission and task assignment, unit movement, communication, malware spread, and defensive strategies in mobile tactical networks is described.

All these IB-models deal with the study of standard malware specimens (computer virures, computer worms, trojans, etc.) and none has appeared addressing the propagation of advanced malware until last year when in [28] a first attempt was done using a cellular automata on graphs to define the dynamics of the model.

Cellular automata are a particular type of finite state machines consisting of n cells: $\mathcal{C} = \{c_i,\, 1 \leq i \leq n\}$, whose connection topology is defined by means of a complex network $\mathcal{G} = (\mathcal{C}, \mathcal{E})$, where $\mathcal{E} \subseteq \mathcal{C} \times \mathcal{C}$ is the set of links between nodes (edges). The set of adjacent cells to a given one $c_i \in \mathcal{C}$ is called its neighborhood and it is denoted by $\mathcal{N}_i = \{c_{\alpha_1}, \ldots, c_{\alpha_i}\}$; moreover, in this work we will suppose that $c_i \notin \mathcal{N}_i$. At time t the cell c_i is endowed with a state s_i^t from a finite state set $\mathcal{S}$, and these states change at discrete steps of time accordingly to a local transition rule f_i which depends on the states of the neighborhood at the previous step of time: $s_i^{t+1} = f_i\left(s_{\alpha_1}^t, \ldots, s_{\alpha_i}^t\right) \in \mathcal{S}$ [29].

As far as we know , and as we said above, only one individual-based model considering advanced malware has been proposed [28]. This is based on a cellu-

lar automata where each memory unit stands for a device and the possible states of these devices can be susceptible, infected and attacked. The transition rules are very simple and they are defined by means of probabilistic coefficients. The main goal of this work is to improve the last mentioned model by considering more realistic assumptions. For example, an additional compartment is added, the recovered devices, since the stealthy behavior of the malware can make it possible to completely ignore some devices once the malicious code has performed its activity on them. Moreover, an evaluation period is now considered; during it malware evaluates the infected host in order to decide its destiny: to be attacked or not, for example.

This work is organized as follows: the detailed description of the novel model for malware propagation is shown in section 2; in section 3 an analysis of the main characteristics and properties of the proposed model is introduced and finally, the conclusions are presented in section 4.

2. Description of the model for advanced malware propagation

Considering the main properties of advanced malware introduced in the last section we will define a model with the following characteristics: (1) this is a compartmental model such that the population of devices remains constant over time and it is divided into four classes: susceptibles (S) -devices which are free of malware-, infected (I) -devices reached by malware-, attacked (A) -devices that have been effectively attacked by malware-, and recovered (R) -devices recovered from advanced malware-; (2) It is an individual-based model since particular characteristics of devices will be taken into account; (3) This is a stochastic model since the transition between some states depend on probabilistic parameters; and (4) as the variables involved in the model (time, states, etc.) are discrete, so is the model.

The dynamics of the proposed model is illustrated in Figure 1. Susceptible devices become infectious when the malware specimen reaches them. To achieve this goal two conditions are necessary: (i) the device should be of interest for

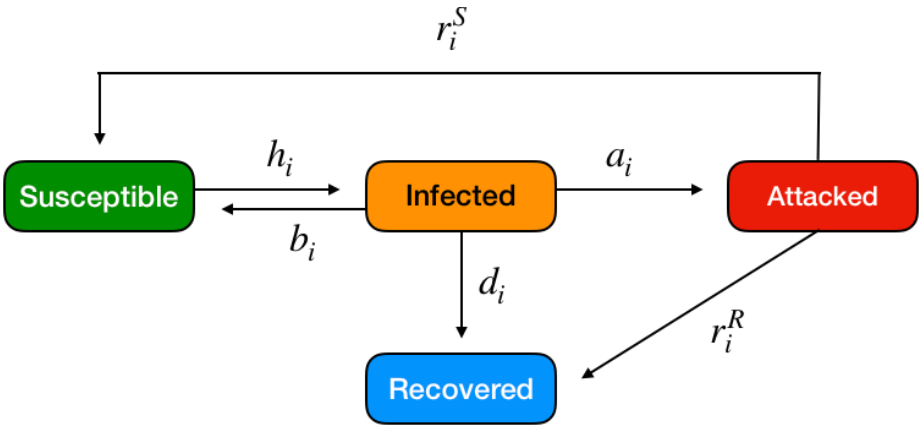

Figure 1: Flow diagram representing the dynamics of the model.

malware either because it can serve as a transmission vector to get the attacked device or because it is one of the targets, and (ii) malware is able to circumvent the security measures implemented in the device. Consequently the susceptible device c_i becomes infectious with probability h_i which is called infection rate.

Once malware has infected a device, it has to analyze this device and decide whether to attack it or not. This is performed over a period of time called evaluation period t_i and, as a consequence of this malware analysis, the infected host device c_i becomes attacked at rate a_i, becomes susceptible at rate b_i, or becomes recovered at rate d_i ($a_i + b_i + d_i = 1$). Note that if the device is not attacked then it could be considered of interest in the future (the host becomes susceptible) or not (in this case it becomes recovered).

Finally, an attacked device c_i remains in this state during a certain period of time τ_i (attack period). Once the advanced malware has executed its malicious payload it removes itself and the attacked device becomes susceptible at rate r_i^S if c_i could be of interest for malware in the future, or it becomes recovered at rate $r_i^R = 1 - r_i^S$ if acquires permanent immunity. In Table 1 a brief description of the epidemiological coefficients involved in the model is introduced.

The dynamics of the model will be governed by means of a probabilistic cellular automaton where the cells stand for the devices and the local interactions

Table 1: Coefficients of the model.

Symbol	Description	Range	Example value
h_i	infection rate	$[0, 1]$	0.25
a_i	attacked coefficient	$[0, 1]$	0.1
b_i	recovery rate (from infected)	$[0, 1]$	0.5
d_i	immunity coefficient (from infected)	$[0, 1]$	0.4
r_i^S	recovery rate (from attacked)	$[0, 1]$	0.4
r_i^R	immunity coefficient (from attacked)	$[0, 1]$	0.6
t_i	evaluation period (hours)	$[1, 24]$	4
τ_i	attack period (hours)	$[12, 72]$	12

defining the neighborhoods will be given by means of random complex networks. Furthermore, the state set will be $\mathcal{S} = \{S, I, R, A\}$. If s_i^t stands for the state of the device c_i at step of time t and Ω_i^t represents the number of infectious neighbor devices of c_i at t, then the local transition functions are the following:

- Transition rule from susceptible to infectious: if $s_i^t = S$ then $s_i^{t+1} = I$ with probability $h_i \cdot \Omega_i^t$.
- Transition rule from infected to attacked: if $s_i^t = I$ and $\tilde{t}_i\,(t) = t_i + 1$ then $s_i^{t+1} = A$ with probability a_i, where $\tilde{t}_i\,(t)$ stands for the time passed in the infected state at t. Otherwise (that is, if $s_i^t = I$ and $\tilde{t}_i\,(t) \leq t_i$) the host c_i remains infected at step of time $t + 1$.
- Transition rule from infected to susceptible: if $s_i^t = I$ and $\tilde{t}_i\,(t) = t_i + 1$ then $s_i^{t+1} = S$ with probability b_i. Otherwise, c_i remains infected until $\tilde{t}_i\,(t) > t_i$.
- Transition rule from infected to recovered: if $s_i^t = I$ and $\tilde{t}_i\,(t) = t_i + 1$ then $s_i^{t+1} = R$ with probability $d_i = 1 - a_i - b_i$. Otherwise, the host remains infected.

- Transition rule from attacked to susceptible (resp. recovered): if $s_i^t = A$ and $\tilde{\tau}_i(t) = \tau_i + 1$ then $s_i^{t+1} = S$ with probability r_i^S (resp. $r_i^R = 1 - r_i^S$). Otherwise, when $\tilde{\tau}_i(t) \leq \tau_i$, then the host remains attacked.

Finally note that recovered devices at a particular step of time remains recovered at the next steps of time, that is, if $s_i^t = R$ then $s_i^{t+1} = R$.

The data flow diagram of the algorithm describing the change of states of a particular device c_i is shown in Figure 2. Note that the following random variables are considered:

$$X = \begin{cases} 1, & \text{with probability } h_i\Omega_i^t \\ 0, & \text{with probability } 1 - h_i\Omega_i^t \end{cases} \quad (1)$$

$$Y = \begin{cases} 0, & \text{with probability } a_i \\ 1, & \text{with probability } b_i \\ 2, & \text{with probability } 1 - a_i - b_i \end{cases} \quad (2)$$

$$Z = \begin{cases} 1, & \text{with probability } r_i^S \\ 0, & \text{with probability } 1 - r_i^S \end{cases} \quad (3)$$

3. Study of the model

3.1. Random complex networks

In this section we will study the behavior of the model when the contact topology is defined by means of a random complex network. The typical model for this type of complex networks is that one defined by Erdös and Rényi [30] and called ER random network model. The algorithm proposed to construct this type of networks is as follows: given a set of n isolated nodes, connect each pair of nodes with an edge with a certain probability $0 < p \leq 1$. Note that as larger the probability p is, the larger the density of the network will be; in this sense for $p = 1$ the complete network will be obtained.

ER random complex networks exhibit some interesting structural properties. For example, there exists a certain threshold value for p, $p_c \sim \frac{\log(n)}{n}$, such

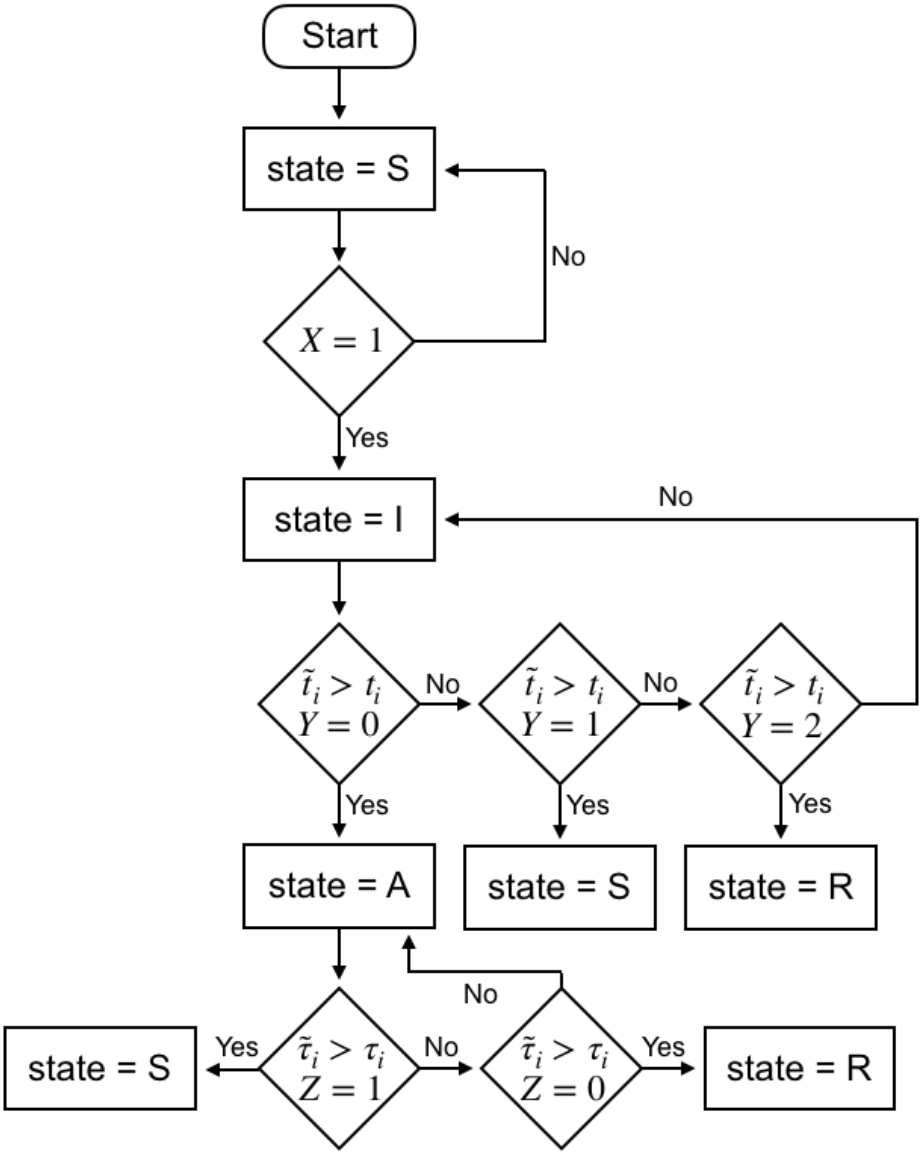

Figure 2: Data flow diagram of the algorithm that defines the change of states of each device.

that when $p \geq p_c$ the network obtained using the last mentioned algorithm is connected. Furthermore, for this networks the node average degree is $\langle k \rangle = p\,(n-1)$, the average path length is $L \sim \frac{\log(n)}{\log(\langle k \rangle)}$, and the clustering coefficient is given by $C \approx \frac{\langle k \rangle}{n} = p$.

3.2. Illustrative numerical simulation

In what follows we will illustrate the model proposed in the last section with a simple simulation. For the sake of simplicity it is supposed that the epidemiological coefficients considered are the same for all devices and their numeric values are shown in Table 1 (last column). Moreover, in this case the number of devices is $n = 50$ and the first 24 hours after the outbreak will be simulated. The random complex network will be defined by the Erdös-Rényi algorithm with probability $p = 0.1$ and there will be only one infected device at step of time $t = 0$ given by the node with highest degree centrality (node in orange in Figure 3 defined in this case by c_{16}). The global evolution of the system is introduced in Figure 4, whereas the individual evolution of each device is shown in Figure 5 where each column stands for the temporal state evolution of each device.

This simulation and the others shown in the following sections have been performed using the software `Mathematica` (version 11.2.0.0) on a 3 GHz Intel Xenon W –64 GB 2666 MHz DDR4–.

3.3. Analysis of the model in the homogeneous case

In this subsection we will study the behavior of the model in the homogeneous case, that is, when some initial structural conditions are varied but considering the epidemiological coefficients as constants (as stated in Table 1). Specifically, different contact topologies will be considered and different choices of the initially infected device (at step of time $t = 0$) will be made. For the sake of simplicity only illustrative examples of the simulations are shown in this work (for each case the behaviors exhibited by the malware spread are similar).

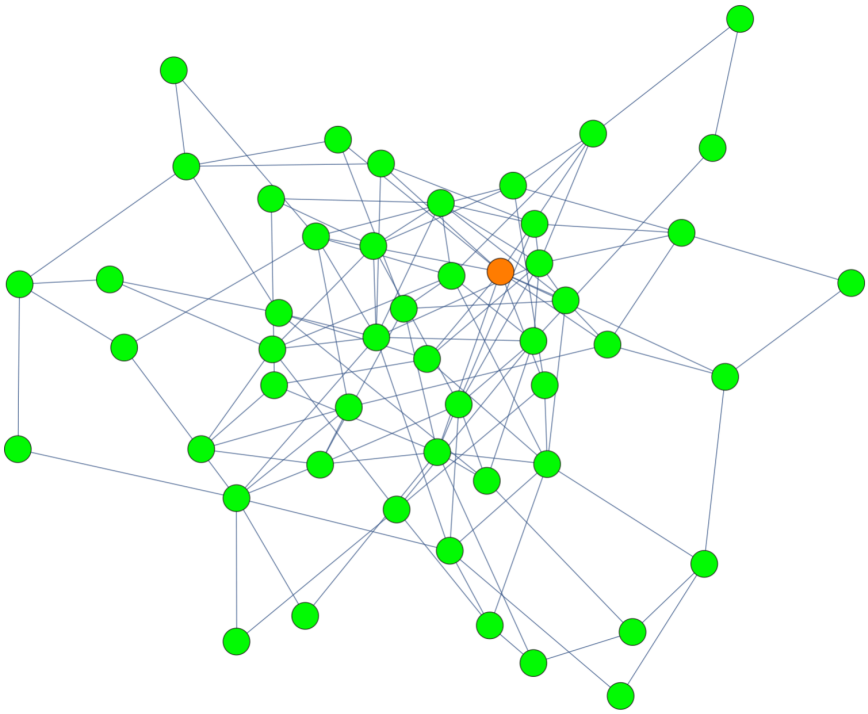

Figure 3: Random complex network defining the contact topology.

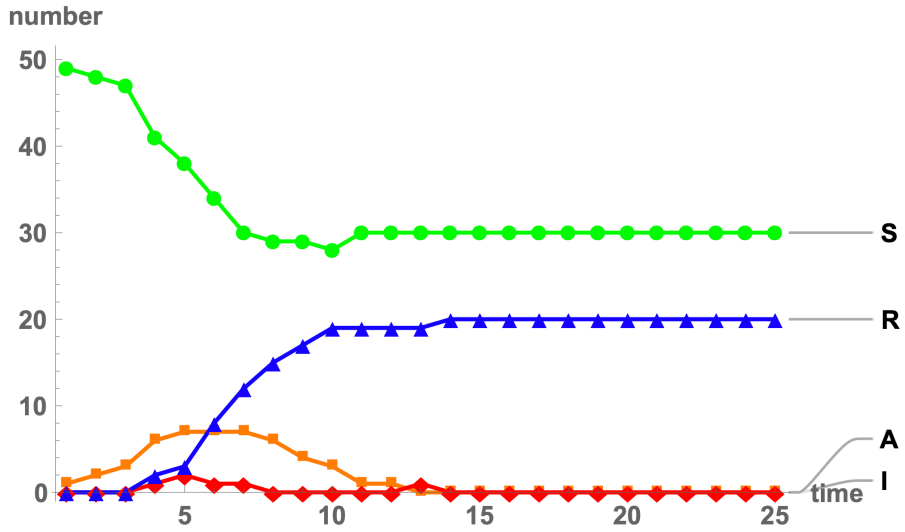

Figure 4: Global evolution (susceptible in green, infected in orange, attacked in red, and recovered in blue)

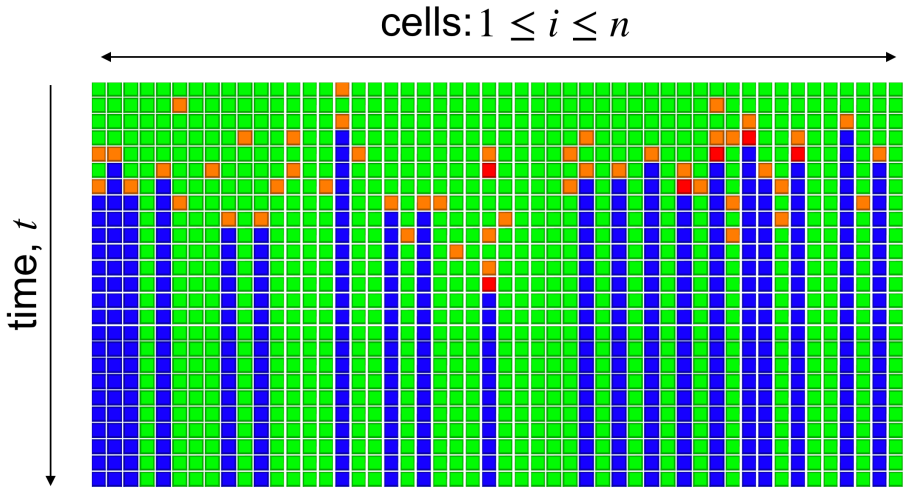

Figure 5: Individual evolution of the states of the devices

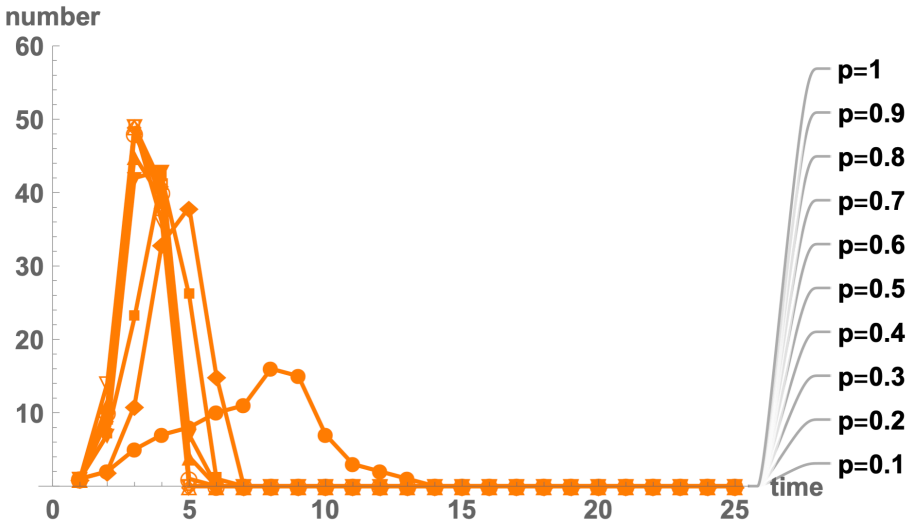

Figure 6: Evolution of infected devices over different ER random complex networks.

In the first case we will examine the behavior of the dynamics of the model when contact topology changes supposing that the epidemiological coefficients remain constant for every device. In addition, as in the previous example, $n = 50$, $0 \leq t \leq 24$ and the unique infected device at $t = 0$ will be the highest degree node. The 10 random complex networks defining the contact topology will be given by the ER algorithm considering $p = 0.1, 0.2, 0.3, \ldots, 0.9, 1$.

The simulations obtained are introduced in Figure 6. Specifically, the evolution of infected devices are shown in Figure 6 whereas the dynamics of the number of attacked devices is shown in Figure 7.

Note that the structure of the network has a great influence in the evolution of the number of infected and attacked devices. Basically the behaviour of both compartments is the same and as higher the probability p is, the higher the maximum number of infected/attacked will be and sooner it will be reached; that is, the propagation speed directly depends on the probability p.

On the other hand, suppose that the epidemiological coefficients and the contact topology is fixed. As in the previous cases, the coefficients involved

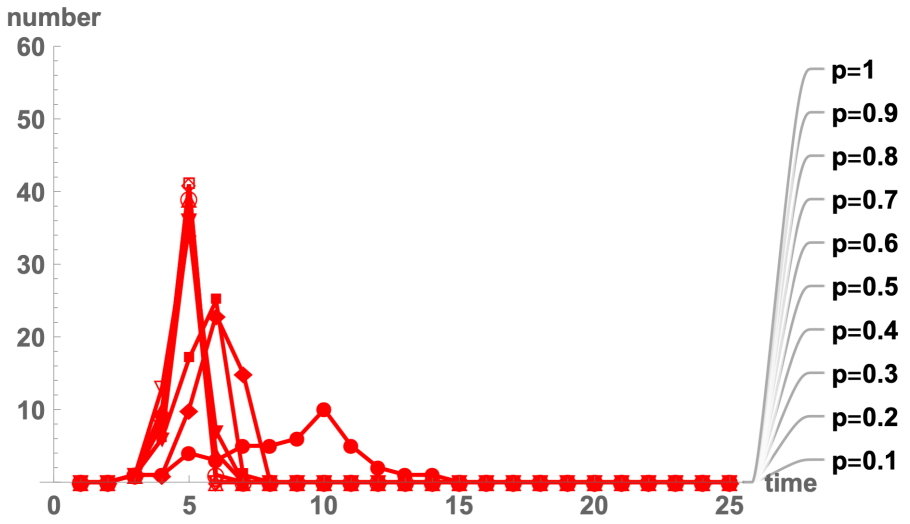

Figure 7: Evolution of attacked devices over different ER random complex networks.

in the model follows the statements introduced in Table 1 whereas the contact topology is defined by an ER random model for $p = 0.1$. Suppose that the infected device at step of time $t = 0$ is chosen taken into account its structural characteristics. For example the nodes with highest centrality measures (degree centrality, closeness centrality, betweenness centrality and eigenvector centrality) will be selected (see Figure 8).

The simulations obtained in this case show that the cyber-attack is most effective (that is, the number of infected/attacked devices rapidly grows and reaches high values) when the initially infected host is chosen considering the highest eigenvector centrality. Furthermore, against what you might think, devices with highest degree values are not the best option as efficient transmission vectors. As is shown in Figure 9 (and in the rest of several simulations computed during the work) the effectiveness of initially infected nodes with the highest closeness centrality or betweenness centrality is greater than this infected node at $t = 0$ with highest degree centrality. Same results are obtained when the evolution of attacked nodes is analyzed (see Figure 10).

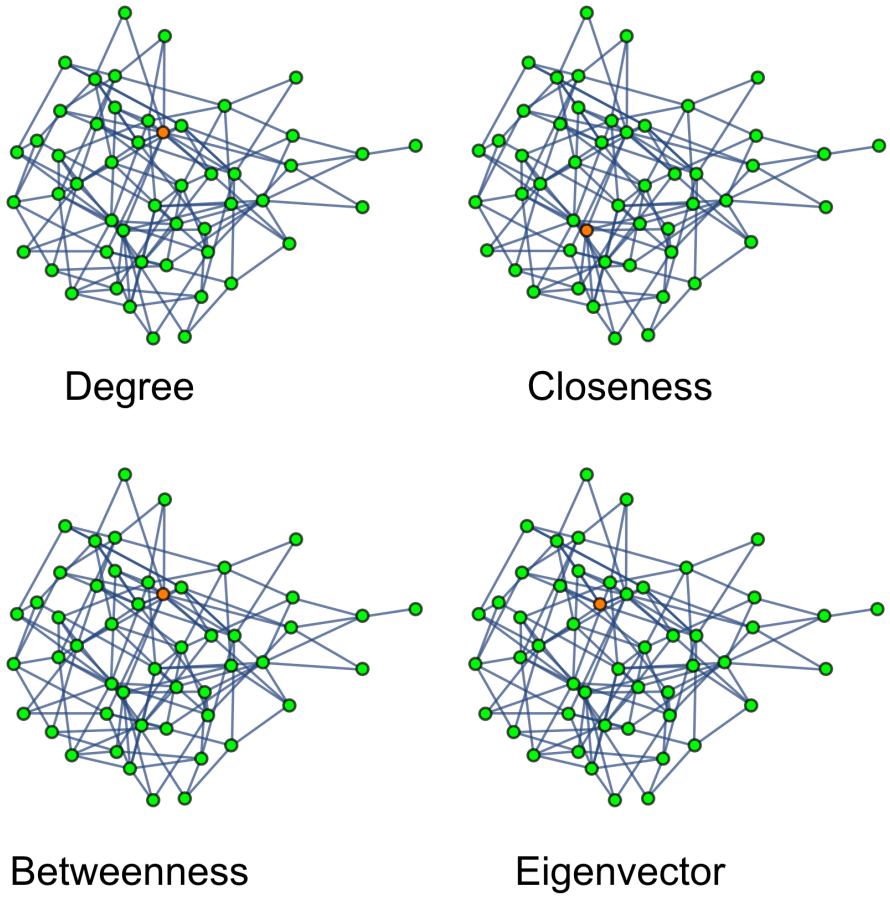

Figure 8: Nodes infected (in orange) at step of time $t = 0$ defined by different centrality measures.

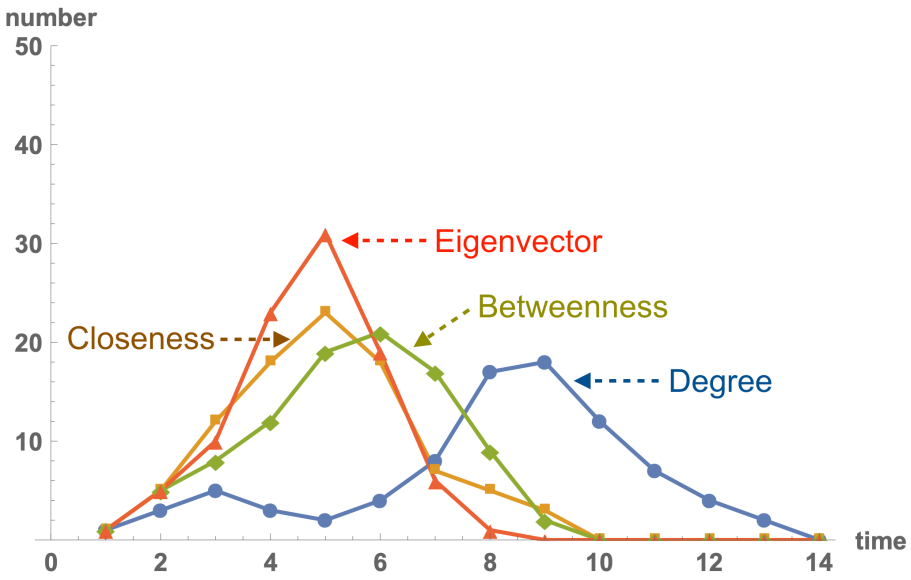

Figure 9: Evolution of infected devices considering different initial infected nodes.

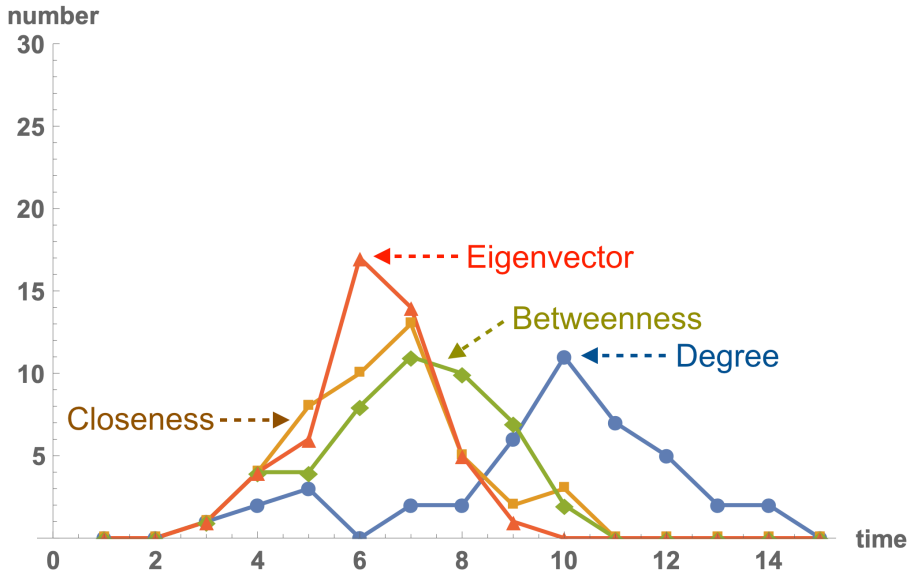

Figure 10: Evolution of attacked devices considering different initial infected nodes.

Table 2: General parameters of the heterogeneous case.

Symbol	Description	Example value
n	number of devices	50
t_{end}	simulation time period (hours)	24
p	Erdös-Rényi probability algorithm	0.5
c_{zero}	zero patient	highest degree centrality

3.4. Analysis of the model in the heterogeneous case

In this subsection more realistic simulations will be performed considering different epidemiological coefficients for each device. Specifically, we will suppose that these coefficients depend on some structural network characteristics associated to the nodes (centrality measures); then we state the following:

(1) The infection rate h_i depends on the clustering coefficient of node c_i, $0 \leq C_{CL}(c_i) \leq 1$, and the virulence of the advanced malware specimen, $0 \leq \eta \leq 1$, so that $h_i = \eta \cdot C_{CL}(c_i)$.

(2) The attacked coefficient associated to device c_i depends on the global importance of the node; as a consequence it can be given by the eigenvector centrality $0 \leq C_E(c_i) \leq 1$: $a_i = C_E(c_i)$.

(3) It is assumed that the rest of coefficients are the same for all devices (see Table 1).

As a consequence, taking into account all these assumptions and considering a environment defined by the parameters given in Table 2 the simulations obtained are shown in Figure 11 and Figure 12. Note that in this case, the system evolves to a disease-free steady state (that is, the number of infected -and attacked- devices disappear).

3.5. Some ideas about security countermeasures

From both qualitative and quantitative point of views, security countermeasures are related to the definition of the recovery rate b_i, due to the characteris-

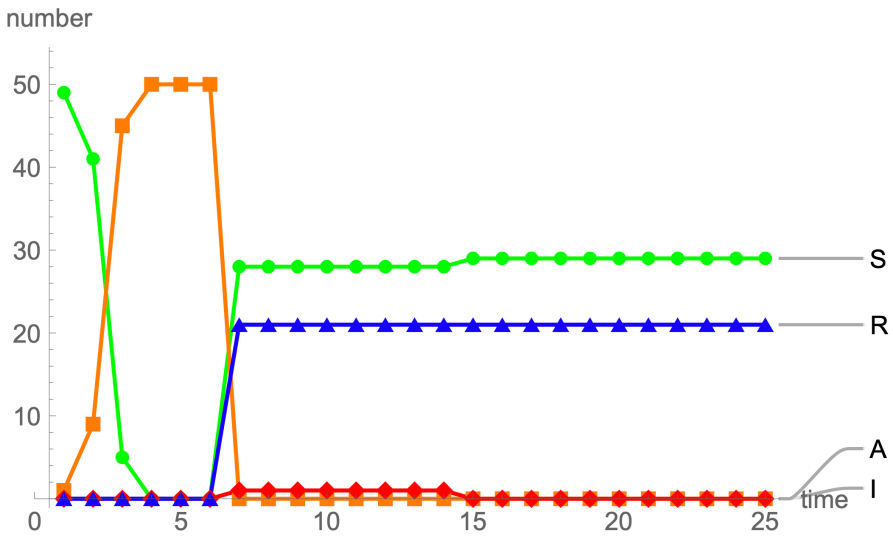

Figure 11: Global evolution of the model.

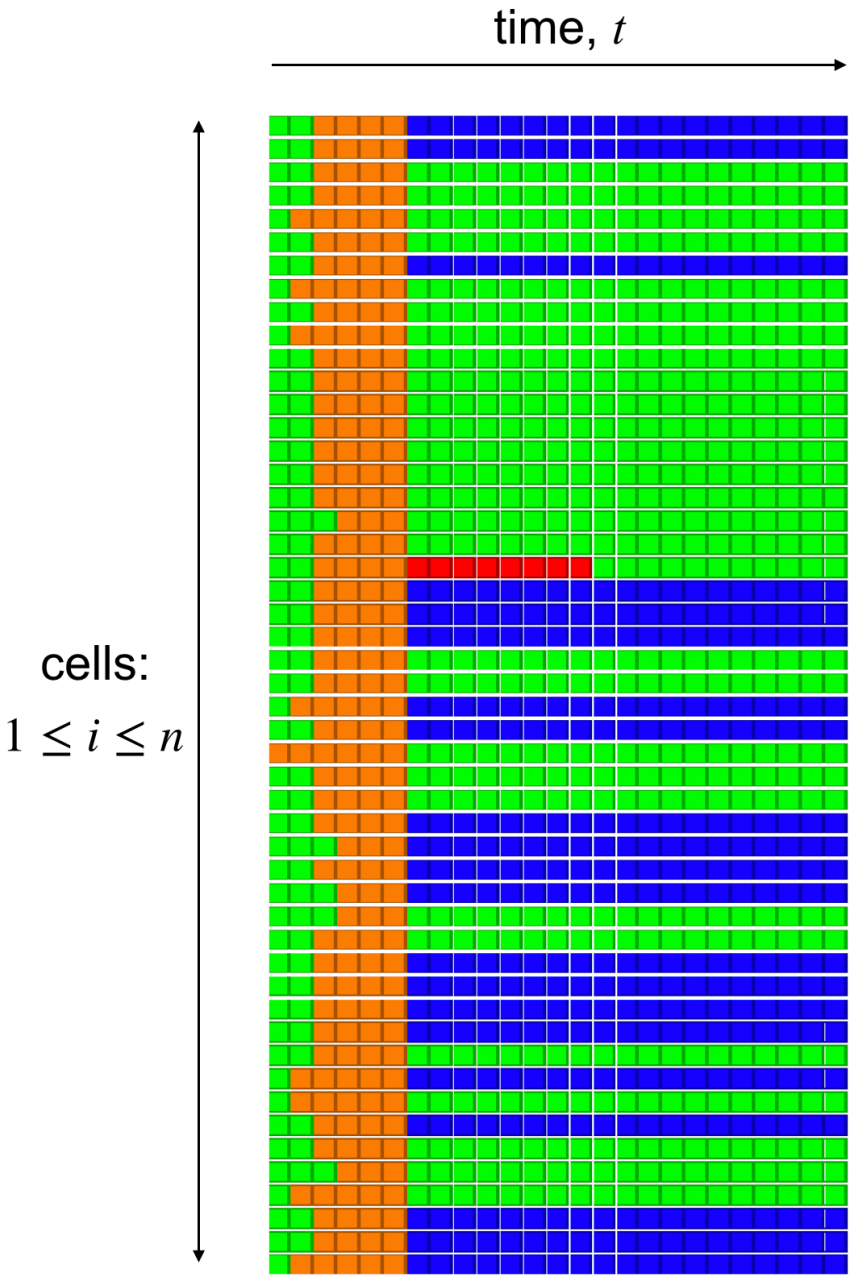

Figure 12: Individual evolution of network devices.

tics of advanced malware. The numeric value of recovery rate could depend on normalized betweenness centrality, C_B, of the associated node (and, possibly, another suitable structural indices). In this case, they can define as follows:

$$b_i = \epsilon \cdot \frac{2 \cdot C_B\left(c_i\right)}{\left(n-1\right)\left(n-2\right)}, \tag{4}$$

where ϵ stands for a coefficient measures the awareness for security of the user of device c_i.

A simple simulation of this new definition of the recovery rate is given in Figure 13. In this case a complete contact topology is considered (that is, the probability of the ER random model is $p = 1$) and the structural and epidemiological coefficients are the same than in the previous examples). In Figure 13-(a) the global evolution of the system is illustrated when $b_i = 0.5\, 1 \leq i \leq n$, whereas in Figure 13-(b) the global evolution of the systems is shown when the recovery coefficient is defined as given in equation (4). Note that in the second case, no attacked devices appear.

4. Conclusions

In this work a novel epidemiological individual-based model to predict the behavior of advanced malware has been described and studied. Specifically, it is a compartmental model where the devices are classified into four compartments: susceptible, infected, attacked and recovered. The dynamics of the model is governed by means of a probabilistic cellular automata and the contact topology is defined by an ER random complex network. Moreover, this model captures the stealthy and evasive behavior of advanced malware.

Although several simulations have been performed during the study, for the sake of simplicity only few illustrative examples are shown in the paper. The following conclusions are derived from the analysis of these simulations:

(1) The probability that defines the ER random model has a direct influence on the propagation process, that is, the malware outbreak can be accelerated or decelerated depending on the value of this probability;

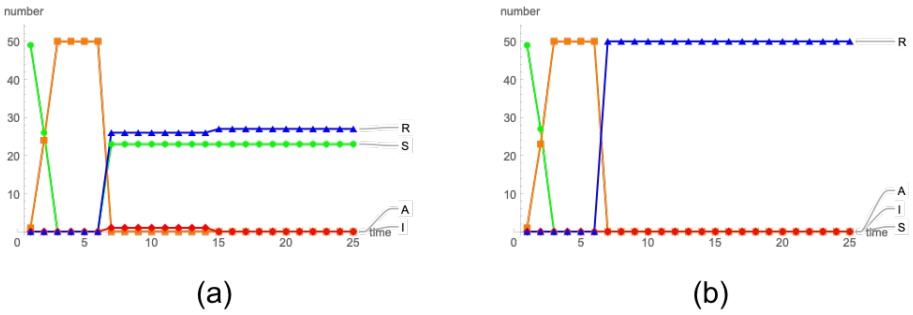

Figure 13: (a) Global evolution with a constant recovery rate. (b) Global evolution of considering a recovery rate depending on the betweenness centrality.

(2) The choice of the first infected device greatly determines the evolution of the number of infected and attacked devices; specifically, the most efficient malware outbreaks are obtained when nodes with the highest eigenvector centrality are firstly attacked.

(3) The implementation of efficient control measures could depend on the computation of some structural network characteristics associated to nodes. For example, the recovery coefficient from infected devices, $b_i\, 1 \leq i \leq n$, could depend on the normalized betweenness centrality.

Future work aimed at validating this theoretical model considering a real environment with real data of both, devices and malware characteristics. Moreover, also the model must be improved using the ABM paradigm. Obviously, an agent-based model is more powerful than a cellular automata model since one can exploit in a more efficient way the AI characteristics of each device (node of the complex network). In this sense, the possibilities of communication and interaction between nodes and the digital environment will provide a more realistic simulation.

Acknowledgements

This research has been partially supported by Ministerio de Ciencia, Innovación y Universidades (MCIU, Spain), Agencia Estatal de Investigación (AEI, Spain), and Fondo Europeo de Desarrollo Regional (FEDER, UE) under project with reference TIN2017-84844-C2-2-R (MAGERAN) and the project with reference SA054G18 supported by Consejería de Educación (Junta de Castilla y León, Spain).

References

[1] A. Ahmad, J. Webb, K.C. Desouza, J. Boorman, Strategically-motivated advanced persistent threat: Definition, process, tactics and a disinformation model of counterattack, Comput. Secur. 86 (2019) 402–418.

[2] W. Tounsi, H. Rais, A survey on technical threat intelligence in the age of sophisticated cyber attacks, Comput. Secur. 72 (2018) 212–233.

[3] A. Lemay, J. Calvet, F. Menet, J.M. Fernandez, Survey of publicly available reports on advanced persistent threat actors, Comput. Secur. 72 (2018) 26–59.

[4] V. Karyotis, M.H.R. Khouzami, Malware Diffusion Models for Modern Complex Networks, Morgan Kaufmann Publishers, Cambridge, MA, 2016.

[5] J.N.C. Goncalves, H.S. Rodrigues, M.T.T. Monteiro, Optimal control measures for a susceptible-carrier-infectious-susceptible malware propagation model, Optim. Control Appl. Methods 40(4) (2019) 691–702.

[6] Y. Connolly, D.S. Wall, 2019. The rise of crypto-ransomware in a changing cybercrime landscape: Taxonomising countermeasures, Comput. Secur. 87, Article number 101568.

[7] W. Gleissner, A mathematical theory for the spread of computer viruses, Comput. Secur. 8 (1989) 35–41.

[8] A. Martín del Rey, Mathematical Modeling of the Propagation of Malware: A Review, Secur. Comm. Netw. 8 (2015) 2561-2579.

[9] S. Peng, S. Yu, A. Yang, Smartphone malware and its propagation modeling: A survey, IEEE Commun. Surv. Tutor. 16(2) 925–941.

[10] A. Al Kindi, D. Al Abri, A. Al Maashri, F. Bait-Shiginah, 2019. Analysis of malware propagation behavior in Social Internet of Things, Int. J. Commun. Syst. 32(15) e4102.

[11] P. Eder-Neuhauser, T. Zseby, J. Fabini, Malware propagation in smart grid networks: metrics, simulation and comparison of three malware types, J. Comput. Virol. 15(2) 109–125.

[12] J.D. Hernández Guillén, A. Martín del Rey, Modeling malware propagation using a carrier compartment, Commun. Nonlinear Sci. Numer. Simul. 56 (2018) 217–226.

[13] S. Hosseini, M.A. Azgomi, A model for malware propagation in scale-free networks based on rumor spreading process, Comput. Netw. 108 (2017) 97–107.

[14] S. Hosseini, M.A. Azgomi, The dynamics of a SEIRS-QV malware propagation model in heterogeneous networks, Physica A 512 (2018) 803–817.

[15] W. Liu, S. Zhong, A novel dynamic model for web malware spreading over scale-free networks, Physica A 505 (2018) 848–863.

[16] C. Zhang, J. Peng, J. Xiao, 2019. An Advanced Persistent Distributed Denial-of-Service Attacked Dynamical Model on Networks. Discrete Dyn. Nat. Soc. 2019, Article ID 2051489.

[17] C. Zhang, J. Xiao, Stability Analysis of an Advanced Persistent Distributed Denial-of-Service Attack Dynamical Model. Secur. Commun. Netw. 2018, Article ID 5353060.

[18] J.D. Hernández Guillén, A. Martín del Rey, R. Casado Vara, Security countermeasures of a SCIRAS model for advanced malware propagation, IEEE Access 7 (2019) 135472-135478.

[19] M. Kotyrba, E. Volna, P. Bujok, Unconventional modelling of complex system via cellular automata and differential evolution, Swarm Evol. Comput. 25 (2015) 52–62.

[20] E.G. Nepomuceno, R.H.C. Takahashi, L.A. Aguirre, Individual-based model (IBM): An alternative framework for epidemiological compartment models, Rev. Bras. Biom. 34(1) (2016) 133–162.

[21] S. Hosseini, M.A. Azgomi, A.R. Torkaman, Agent-based simulation of the dynamics of malware propagation in scale-free networks, Simulation 92(7) (2016) 709–722.

[22] A. Bose, K.G. Shin, Agent-based modeling of malware dynamics in heterogeneous environments, Secur. Commun. Netw. 6(12) (2013) 1576–1589.

[23] Y. Wang, D. Li, N. Dong, Cellular automata malware propagation model for WSN based on multi-player evolutionary game, IET Netw. 7(3) (2018) 129–135.

[24] Y.R. Song, G.P. Jiamg, Malware propagation in scale-free networks for the nodes with different anti-attack abilities, Acta Phys. Sin. 59(2) (2010) 705-711.

[25] Y.R. Song, G.P. Jiamg, Research of malware propagation in complex networks based on 1-D cellular automata, Acta Phys. Sin. 58(9) (2009) 5911-5918.

[26] P. Hu, L. Ding, T. Hadzibeganovic, Individual-based optimal weight adaptation for heterogeneous epidemic spreading networks, Commun. Nonlinear Sci. Numer. Simul. 63 (2018) 339–355.

[27] B. Thomson, J. Morris-King, An agent-based modeling framework for cybersecurity in mobile tactical networks, J. Def. Model. Simulat. 15 (2018) 204–218.

[28] A. Martín del Rey, A. Queiruga Dios, G. Hernández, A. Bustos Tabernero, Modeling the Spread of Malware on Complex Networks, in: E. Herrera-Viedma *et al.* (Eds.), Distributed Computing and Artificial Intelligence, 16th International Conference, Special Sessions. DCAI 2019. Advances in Intelligent Systems and Computing, vol 1004. Springer, Cham, 2020, pp. 109–116.

[29] P. Sarkar, A brief history of cellular automata, ACM Comput. Surv. 32 (2000) 80–107.

[30] P. Erdös, A. Rényi, On the evolution of random graphs, Publications of the Mathematical Institute of the Hungarian Academy of Science 5 (1960) 17–60.