Modeling malware propagation using a carrier compartment

J.D. Hernández Guillén[a], A. Martín del Rey[b]

[a] *University of Salamanca, Department of Applied Mathematics*
Calle del Parque 2, 37008-Salamanca, Spain
E-mail: diaman@usal.es
[b] *(Corresponding author)*
University of Salamanca
Institute of Fundamental Physics and Mathematics
Department of Applied Mathematics
Calle del Parque 2, 37008-Salamanca, Spain
E-mail: delrey@usal.es

Abstract

The great majority of mathematical models proposed to simulate malware spreading are based on systems of ordinary differential equations. These are compartmental models where the devices are classified according to some types: susceptible, exposed, infectious, recovered, etc. As far as we know, there is not any model considering the special class of carrier devices. This type is constituted by the devices whose operative systems is not targeted by the malware (for example, iOS devices for Android malware).

In this work a novel mathematical model considering this new compartment is considered. Its qualitative study is presented and a detailed analysis of the efficient control measures is shown by studying the basic reproductive number.
Keywords: Malware propagation, Carrier devices, Basic reproductive number, Stability

1. Introduction

Malware is one of the most important tools used in cybersecurity attacks, and this fact has been reaffirmed in the last years with the appearance of zero-days attacks and advanced persistent threats ([1, 2]). The risks associated to these cyberattacks in the new paradigms as the Internet of Things ([3, 4]) and

Industry 4.0 ([5, 6]) are enormous and, consequently, this threat must be properly managed.

Although the scientific approach to combat malware is mainly focused on the design of efficient methods to detect all types of malware ([7]), the design and computational implementation of mathematical models to simulate its spreading is also a very important task. These models allow us not only to predict the behavior of the evolution of malware, but also to study the efficacy of different possible countermeasures. As a consequence, these analytical tools could play a very important role in the forensic computing and cybercrime investigation.

The great majority of the mathematical models for malware spreading that have been proposed in the scientific literature are compartmental, global, complete and deterministic ([8, 9]).

They are compartmental models since the devices are divided into some types (or compartments) according to their status: susceptible (S), exposed (E), infectious (I), recovered (R), vaccinated (V), immunized (P), damaged (D) etc. As a consequence, and considering the dynamics between these compartments, we obtain different types of models: SI ([10]), SIR ([11]), SEIR ([12]), SEIRS ([13, 14, 15]), SVEIR ([16, 17]), SIRP ([18]), SED ([19]), etc.

They are global models since each compartment is considered as an unique entity with their own characteristics. Moreover, the dynamics of resources used by these compartments are explicitly represented in the equations of the model. In contrast, individual-based models consider each device as an entity taking into account their particular characteristics and local interactions ([20]).

They can be considered as complete models since it is supposed that the contact topology is defined by means of a complete graph; that is, all devices are in contact with each other all time. On the other hand, network models (based on, for example, scale-free networks) have also recently been proposed ([21, 22]).

Finally, they are deterministic models based on a system of ordinary differential equations. In fact, the temporal evolution of each compartment is ruled by one of these differential equations. The relevance of these models lies on

the fact that the qualitative theory of ordinary differential equations can be used to study the behavior and dynamics of their solutions. On the other hand, stochastic models have also been proposed ([23]).

A detailed analysis of these models based on ordinary differential equations reveals that:

(1) As far as we know, no proposed model considers in its dynamics the devices that can be infected by the malware but cannot be damaged, although they can act as transmission vectors (i.e. they can transmit the infection to susceptible devices). This new type is constituted by the devices whose operative systems is not targeted by the malware (for example, iOS devices for Android malware), and they can be denoted as carrier devices (C).

(2) The analytical study of the basic reproductive number, R_0, (the main threshold parameter which indicates whether a malware outbreak can become epidemic) is basic in order to design efficient control strategies. As far as we know, there is not any profound effort to analyze R_0 based on the epidemiological parameters on which depends. Actually, its study usually depends on an only parameter at most.

Consequently, it is of interest to design new mathematical models that overcome the last mentioned drawbacks. In this sense, the main goal of this work is to proposed a novel mathematical model to simulate malware spreading considering the new class of carrier devices. Moreover, a detailed analysis of the basic reproductive number will be performed in order to obtain efficient control measures that involve several parameters.

The rest of the paper is organized as follows: In section 2 a detailed description of the new mathematical model is presented; the stability analysis of the equilibrium points is introduced in section 3; in section 4 the analysis of the control measures is given, and finally, the conclusions are presented in section 5.

2. New Mathematical Model to Simulate Malware Propagation

2.1. Description of the model

The model proposed in this work is a compartmental model where the population is divided into four classes: susceptible $S(t)$, carrier $C(t)$, infectious $I(t)$, and recovered $R(t)$. Specifically, it is a SCIRS model (i.e., reinfection is considered) with vaccination process and without population dynamics: $S(t) + I(t) + C(t) + R(t) = N > 0$. The dynamics of the model is ruled by means of the following assumptions (see Figure 1):

- Both, carriers and infectious devices, can infect susceptible devices at the same transmission rate a. In this sense, let δ be the fraction of susceptible devices endowed with the targeted operative system. As a consequence $\delta a S(t)(C(t) + I(t))$ stands for the new infectious devices at every step of time. Similarly, $(1-\delta) a S(t)(C(t) + I(t))$ represents the number of new carrier devices at t.

- Susceptible devices can acquire temporal immunity to malware attack according to the vaccination rate v. As a consequence, $vS(t)$ is the number of susceptible devices moved to recovered class at time t.

- If security software successfully detects and removes the malware, carriers and infectious devices acquire temporal immunity at rates b_C and b_I, respectively. Thus, $b_C C(t)$ and $b_I I(t)$ stand for the number of new recovered devices from carrier and infectious compartments respectively.

- Finally, recover devices lose their temporal immunity and turn back to be susceptible compartment at recovery rate ϵ. Consequently, $\epsilon R(t)$ represents the new susceptible devices at time t.

Considering these assumptions, the dynamics of the model is governed by means of the following system of ordinary differential equations:

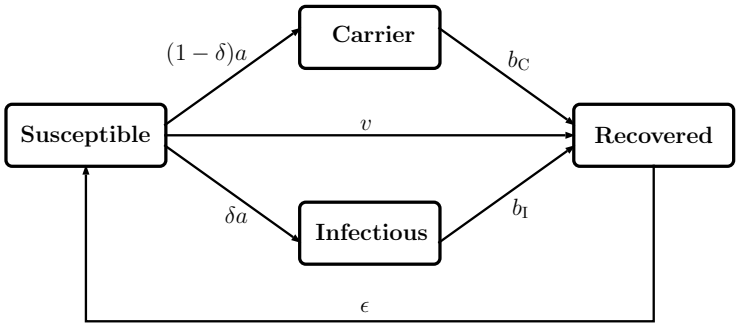

Figure 1: Flow diagram representing the dynamics of the SCIRS model.

$$\begin{aligned}
\frac{dS(t)}{dt} &= \epsilon R(t) - aS(t)(I(t)+C(t)) - vS(t), && (1)\\
\frac{dC(t)}{dt} &= a(1-\delta)S(t)(I(t)+C(t)) - b_C C(t), && (2)\\
\frac{dI(t)}{dt} &= a\delta S(t)(I(t)+C(t)) - b_I I(t), && (3)\\
\frac{dR(t)}{dt} &= b_C C(t) + b_I I(t) + vS(t) - \epsilon R(t). && (4)
\end{aligned}$$

2.2. Existence and uniqueness of the solutions of the model

As $S(t)+C(t)+I(t)+R(t)=N$ the system (1)-(4) can be written as follows:

$$\begin{aligned}
\frac{dS(t)}{dt} &= -aS(t)(I(t)+C(t)) - vS(t) + \epsilon(N-S(t)-C(t)-I(t)), && (5)\\
\frac{dC(t)}{dt} &= a(1-\delta)S(t)(I(t)+C(t)) - b_C C(t), && (6)\\
\frac{dI(t)}{dt} &= a\delta S(t)(I(t)+C(t)) - b_I I(t). && (7)
\end{aligned}$$

The feasible region for this system is $\Omega = \{(S,C,I) \in \mathbb{R}_3^+ : 0 \leq S+C+I \leq N\}$, where its boundary $\partial\Omega$ is delimited by four faces:

$$\begin{aligned}
F_1 &= \{(S,C,I) \in \mathbb{R}_3^+ : S+C+I = N \text{ with } 0 \leq S,C,I \leq N\}, && (8)\\
F_2 &= \{(S,C,I) \in \mathbb{R}_3^+ : S = 0 \text{ with } C+I \leq N\}, && (9)\\
F_3 &= \{(S,C,I) \in \mathbb{R}_3^+ : C = 0 \text{ with } S+I \leq N\}, && (10)\\
F_4 &= \{(S,C,I) \in \mathbb{R}_3^+ : I = 0 \text{ with } S+C \leq N\}, && (11)
\end{aligned}$$

such that their outer normal vectors are, respectively, $\vec{n}_1 = (1,1,1)$, $\vec{n}_2 = (-1,0,0)$, $\vec{n}_3 = (0,-1,0)$, and $\vec{n}_4 = (0,0,-1)$. A simple computation shows that:

$$\left(\frac{dS}{dt}, \frac{dC}{dt}, \frac{dI}{dt}\right)_{F_1} \bullet \vec{n}_1 = -b_C C - b_I I - vS \leq 0, \quad (12)$$

$$\left(\frac{dS}{dt}, \frac{dC}{dt}, \frac{dI}{dt}\right)_{F_2} \bullet \vec{n}_2 = (C + I - N)\,\epsilon \leq 0, \quad (13)$$

$$\left(\frac{dS}{dt}, \frac{dC}{dt}, \frac{dI}{dt}\right)_{F_3} \bullet \vec{n}_3 = aIS(\delta - 1) \leq 0, \quad (14)$$

$$\left(\frac{dS}{dt}, \frac{dC}{dt}, \frac{dI}{dt}\right)_{F_4} \bullet \vec{n}_4 = -aCS\delta \leq 0. \quad (15)$$

Now, Ω is compact and invariant since Ω is closed -which implies $\bar{\Omega} = \Omega$- ([10, 24]). As a consequence, the solutions of the system (5)-(7) initiating in the feasible region Ω, exist and are unique for all $t \geq 0$ [25].

2.3. Equilibrium Points

The equilibrium points of the system (1)-(4) can be obtained by solving the following system of non-linear equations:

$$0 = -aS(t)\,(I(t) + C(t)) - vS(t) + \epsilon\,(N - S(t) - C(t) - I(t))\,, \quad (16)$$

$$0 = a(1-\delta)S(t)\,(I(t) + C(t)) - b_C C(t)\,, \quad (17)$$

$$0 = a\delta S(t)\,(I(t) + C(t)) - b_I I(t)\,. \quad (18)$$

It is easy to check that there are two solutions: the disease-free equilibrium point

$$E_0 = (S_0, C_0, I_0) = \left(\frac{\epsilon N}{v + \epsilon}, 0, 0\right), \quad (19)$$

and the endemic equilibrium point

$$E^* = (S^*, C^*, I^*) = \left(\frac{b_C b_I}{J}, \frac{b_I(1-\delta)L}{JK}, \frac{b_C \delta L}{JK}\right), \quad (20)$$

where

$$J = ab_I + ab_C\delta - ab_I\delta, \quad (21)$$

$$K = b_I(1-\delta)\epsilon + b_C(b_I + \delta\epsilon), \quad (22)$$

$$L = ab_I N(1-\delta)\epsilon + b_C(aN\delta\epsilon - b_I(v+\epsilon)). \quad (23)$$

Note that the endemic solution only exists if

$$\frac{aN(b_I + b_C\delta - b_I\delta)\epsilon}{b_C b_I(v+\epsilon)} > 1. \tag{24}$$

2.4. Basic reproductive number

As is well-known, the basic reproductive number, R_0, is an important epidemiological threshold parameter whose numeric value characterizes the behavior of the solutions of the system. The next-generation matrix method [26] is used to calculate it. Through certain computations we obtain that the next-generation matrix at the disease-free equilibrium point is $G = F \cdot V^{-1}$, where:

$$F = \begin{pmatrix} \frac{aN(1-\delta)\epsilon}{v+\epsilon} & \frac{aN(1-\delta)\epsilon}{v+\epsilon} \\ \frac{aN\delta\epsilon}{v+\epsilon} & \frac{aN\delta\epsilon}{v+\epsilon} \end{pmatrix}, \qquad V = \begin{pmatrix} b_C & 0 \\ 0 & b_I \end{pmatrix}. \tag{25}$$

Consequently, the spectral radius of G is the basic reproductive number:

$$R_0 = \frac{aN\left(b_I + b_C\delta - b_I\delta\right)\epsilon}{b_C b_I\left(v+\epsilon\right)}. \tag{26}$$

Note that the condition for the existence of the endemic equilibrium point is, precisely, that $R_0 > 1$.

3. Study of the stability

3.1. Local stability of the equilibrium points

The following results hold dealing with the local stability of the equilibrium points:

Theorem 1. *The disease-free equilibrium point* $E_0 = \left(\frac{\epsilon N}{v+\epsilon}, 0, 0\right)$ *is locally asymptotically stable if* $R_0 < 1$.

Proof. The disease-free equilibrium point is locally asymptotically stable if the eigenvalues of the matrix $F - V$ and $\frac{\partial}{\partial S}\left(-vS + \epsilon\left(N - S\right)\right)$ have all negative real parts (see [27]). Note that the eigenvalues of

$$F - V = \begin{pmatrix} \frac{aN(1-\delta)\epsilon}{v+\epsilon} - b_C & \frac{aN(1-\delta)\epsilon}{v+\epsilon} \\ \frac{aN\delta\epsilon}{v+\epsilon} & \frac{aN\delta\epsilon}{v+\epsilon} - b_I \end{pmatrix} \tag{27}$$

are

$$\frac{b_I^2\left(1-\delta\right)+b_C^2\delta+b_Ib_C\left(1-R_0\right)\pm\sqrt{U}}{2b_I\left(-1+\delta\right)-2b_C\delta}, \tag{28}$$

where

$$\begin{aligned} U &= \left(b_i-b_C\right)^2\left(b_I\left(-1+\delta\right)-b_C\delta\right)^2 \\ &\quad +2b_I\left(b_I-b_C\right)b_C\left(-1+2\delta\right)\left(b_I\left(-1+\delta\right)-b_C\delta\right)R_0+b_I^2b_C^2R_0^2. \end{aligned} \tag{29}$$

A simple computation shows that these eigenvalues have negative real part if $1-R_0>0$, that is, if $R_0<1$. On the other hand $\frac{\partial}{\partial S}\left(-vS+\epsilon\left(N-S\right)\right)=-v-\epsilon<0$, thus finished. □

Theorem 2. *The endemic equilibrium point E^* is locally asymptotically stable if $R_0>1$.*

Proof. The Routh-Hurwitz criterion [28] will be applied to show that the endemic equilibrium E^* is locally asymptotically stable for $R_0>1$. Let $P(\lambda)=p_0\lambda^3+p_1\lambda^2+p_2\lambda+p_3$ be the characteristic polynomial of the Jacobian matrix of system (5)-(7) at endemic-free equilibrium point, then:

$$p_0 = 1, \tag{30}$$

$$p_1 = \frac{a\left(-b_Cb_IK+b_IL+b_CL\delta-b_IL\delta\right)+JK\left(b_C+b_I+v+\epsilon\right)}{JK}, \tag{31}$$

$$\begin{aligned} p_2 &= b_I\left(v+\epsilon\right)+b_C\left(b_I+v+\epsilon\right) \\ &\quad +\frac{a(b_{\mathrm{C}}^2(L-Kb_{\mathrm{I}})\delta-b_{\mathrm{I}}L(\delta-1)(b_{\mathrm{I}}+\epsilon))}{JK} \\ &\quad +\frac{a(b_{\mathrm{C}}(b_{\mathrm{I}}^2K(\delta-1)+L\delta\epsilon+b_{\mathrm{I}}(L-K(v+\epsilon))))}{JK}, \end{aligned} \tag{32}$$

$$p_3 = L. \tag{33}$$

Therefore, by certain calculations we get $p_0>0, p_1>0, p_3>0$, and $p_1p_2-p_3>0$, for $R_0>1$. Consequently, the claimed result follows from Routh-Hurwitz criterion. □

3.2. Global stability of the equilibrium points

3.2.1. Global stability of the disease-free equilibrium point

In this section we will demonstrate the global stability of the disease-free equilibrium point E_0 in Ω. The following result holds:

Theorem 3. *The disease-free equilibrium E_0 is globally asymptotically stable if $R_0 \leq 1$.*

Proof. We will apply the LaSalle invariance principle ([29]) to proof the global stability. According to (5) we have

$$\dot{S} \leq \epsilon N - S(v+\epsilon), \tag{34}$$

$$\dot{X} = \epsilon N - X(v+\epsilon), \tag{35}$$

where X is an auxiliary variable. Using the Comparison Theorem [30] we have that $X(t)$ is an upper solution of $S(t)$, that is, $X(t) > S(t)$ for all $t > 0$. Since $\lim_{t\to\infty} X(t) = (\epsilon N)/(v+\epsilon)$, then

$$S \leq \frac{\epsilon N}{v+\epsilon}, \tag{36}$$

as $t \to \infty$.

Now, if we consider the Lyapunov function $V = b_I C + b_C I$, from inequality (36), we obtain

$$\begin{aligned} \frac{dV}{dt} &= b_I\left(\left(1-\delta\right)S\left(I+C\right) - b_C C\right) + b_C\left(\delta S\left(I+C\right) - b_I I\right) \\ &= \left(b_I\left(1-\delta\right)S + b_C\delta S - b_I b_C\right)C + \left(b_I\left(1-\delta\right)S + b_C\delta S - b_I b_C\right)I \\ &\leq b_I b_C\left(R_0 - 1\right)C + b_I b_C\left(R_0 - 1\right)I. \end{aligned} \tag{37}$$

Note that $\frac{dV}{dt} \leq 0$ holds for $R_0 \leq 1$ and $(S, C, I) \in \Omega$. Furthermore, $\frac{dV}{dt} = 0$ if and only if $(C, I) = (0, 0)$ or $S = (\epsilon N)/\left(v+\epsilon\right)$ and $R_0 = 1$. Here, $(S, I, C) \to E_0$ as $t \to \infty$. Then, the maximum invariant set in $\{(S, C, I) \in \Omega : \frac{dV}{dt} = 0\}$ is the singleton E_0. Finally, the claimed result follows from LaSalle invariance principle [29, Chapter 2, Theorem 6.4] and the explicit expression of the Lyapunov function defined. □

3.2.2. Global Stability of Epidemic Equilibrium

Now we will demonstrate the global stability of the endemic equilibrium point E^* in $\text{int}(\Omega)$ under certain assumptions. Applying the geometrical approach we obtain the following results:

Theorem 4. *The system (5)-(7) is uniformly persistent for $R_0 > 1$.*

Proof. It is easy to check that the system (5)-(7) satisfies the following statements:

- As the vector field of the system is subtangential to Ω for all point of $\partial\Omega$, then Ω is closed and invariant ([24]).
- If $x(t, x_0)$ is a solution of the system initiating in $x_0 = (S(0), C(0), I(0))$, and M is the set of all points belonging to $\partial\Omega$ such that the vector field of the system is tangential to Ω, then $M = \{x_0 \in \partial\Omega : x(t, x_0) \in \partial\Omega \text{ for all } t > 0\}$ is $(C, I) = (0, 0)$. Here, $(S, I, C) \to E^*$ as $t \to \infty$. Furthermore, E_0 is isolated as $R_0 > 1$ (see Theorem 2) and acyclic. Then, N_α is the singleton E^*.

Applying [31, Theorem 4.3] we obtain the claimed result. □

Note that the uniformly persistence of the model implies the existence of an absorbent compact in $\text{int}(\Omega)$ [32]. Moreover, $\text{int}(\Omega)$ is a simply connected set and E^* is the only equilibrium point in $\text{int}(\Omega)$.

Theorem 5. *Under the assumptions*

$$-v - a(1-\delta)\frac{c^2}{N} - 2ac + \frac{a\delta N}{v+\epsilon}(\delta + 2) + \epsilon < 0, \tag{38}$$

$$-b_I - a(1-\delta)\frac{c^2}{N} + \frac{a\delta N\epsilon}{v+\epsilon} + a(2N - 4c)\max\{(1-\delta), \delta\} < 0, \tag{39}$$

where c is the persistence constant, the endemic equilibrium point E^* is globally asymptotically stable if $R_0 > 1$ with respect to solutions of (5)-(7) initiating in $\text{int}(\Omega)$.

Proof. The explicit expression of the second additive compound matrix of Jacobian matrix is

$$J^{[2]} = \begin{pmatrix} -b_C - v - a(I + C - S(1-\delta)) - \epsilon & aS(1-\delta) & aS + \epsilon \\ aS\delta & -b_I - a(C + I) - v + aS\delta - \epsilon & -aS - \epsilon \\ -a(I + C)\delta & a(C + I)(1-\delta) & -b_C - b_I + aS \end{pmatrix}. \tag{40}$$

If

$$A = \text{diag}\left(\frac{S}{C}, \frac{S}{C}, \frac{S}{C}\right) \tag{41}$$

is the diagonal matrix, and A_f stands for the directional derivative of A along (S, C, I), we obtain:

$$A_f \cdot A^{-1} = \text{diag}\left(\frac{1}{S}\frac{dS}{dt} - \frac{1}{C}\frac{dC}{dt}, \frac{1}{S}\frac{dS}{dt} - \frac{1}{C}\frac{dC}{dt}, \frac{1}{S}\frac{dS}{dt} - \frac{1}{C}\frac{dC}{dt}\right). \tag{42}$$

Therefore, the matrix $B = A_f A^{-1} + AJ^{[2]}A^{-1}$ can be written as follows:

$$\begin{pmatrix} G + b_I - v - a\left(I + C - S\left(1-\delta\right)\right) - \epsilon & aS\left(1-\delta\right) & aS + \epsilon \\ aS\delta & G + b_C - a\left(C + I\right) - v + aS\delta - \epsilon & -aS - \epsilon \\ -a\left(I + C\right)\delta & a\left(C + I\right)\left(1-\delta\right) & G + aS \end{pmatrix}, \tag{43}$$

where

$$G = \frac{1}{S}\frac{dS}{dt} - \frac{1}{C}\frac{dC}{dt} - b_C - b_I. \tag{44}$$

According to [33], its Lozinskii measure $\mu(B)$ associated with a norm $||.||$ can be evaluated as follows:

$$\mu(B) = \inf\{c : \mathrm{D}_+||z|| \leq c||z|| \text{ for all solutions of } \dot{z} = Bz\}, \tag{45}$$

where D_+ is the right-hand derivative [34, 35]. Moreover, if we define the norm of $z = (z_1, z_2, z_3)$ as $||z|| = \max\{||z_1|| + ||z_2||, ||z_3||$, it is possible to estimate $\mathrm{D}_+||z||$ through two cases:

- If $||z|| = ||z_1|| + ||z_2||$, then:

$$\mathrm{D}_+||z|| \leq \left(\frac{1}{S}\frac{dS}{dt} - a\left(1-\delta\right)S\frac{I}{C} - v - a\left(I + C\right) + aS\delta + 2aS + \epsilon\right)||z||. \tag{46}$$

- If $||z|| = ||z_3||$, then:

$$\mathrm{D}_+||z|| \leq \left(\frac{1}{S}\frac{dS}{dt} - b_I - a\left(1-\delta\right)\frac{SI}{C} + as\delta + a\left(C + I\right)\max\{\left(1-\delta\right), \delta\}\right)||z||. \tag{47}$$

Taking into account the equations (45)-(47) and the assumptions (38) and (39), we have

$$\mu(B) \leq \frac{1}{S}\frac{dS}{dt} - \theta, \tag{48}$$

with $\theta > 0$. Then, there exists a constant $T > 0$ such that $t > T$ implies $I(t) < e^{(\theta t/2)}$ and, thus

$$\frac{1}{t}\log S(t) < \frac{\theta}{2} \tag{49}$$

along each solution of system (5)-(7) in $\text{int}(\Omega)$. For big enough t, we have

$$\overline{q}_2 = \limsup_{t\to\infty} \sup_{(S(0),C(0),I(0))\in\text{int}(\Omega)} \frac{1}{t}\int_0^t \mu(B)dt < -\frac{1}{2}\theta < 0, \tag{50}$$

thus finishing applying the geometrical approach [36]. □

3.3. Numerical simulations

Suppose that there are 1001 devices in the network such that initially all devices are susceptible with the exception of only one that is infectious: $S(0) = 1000, I(0) = 1, C(0) = R(0) = 0$. Moreover, set $a = 0.0002$, $\epsilon = 0.004$, $b_C = 0.004$, $b_I = 0.03$ and $\delta = 0.9$. Moreover, the time is measured in hours and the simulation period comprises the first two weeks (336 hours) after the onset of the first infectious device.

3.3.1. Disease-free steady state

If we suppose that $v = 0.05$ then $R_0 \approx 0'81563 \leq 1$ and consequently the number of infected computers does not increase. This behavior is shown in Fig. 2. Moreover, the system reaches the following disease-free steady state:

$$E_0 = (S_0, C_0, I_0, R_0) \approx (74'1481, 0, 0, 926'852). \tag{51}$$

3.3.2. Endemic steady state

On the other hand, if we set $v = 0.01$ then $R_0 \approx 3'146 > 1$ and consequently the outbreak becomes epidemic as it is shown in Fig.3. Furthermore, the endemic steady state is given by the following values:

$$E^* = (S^*, C^*, I^*, R^*) \approx (90'9091, 55'9687, 67'1624, 786'96). \tag{52}$$

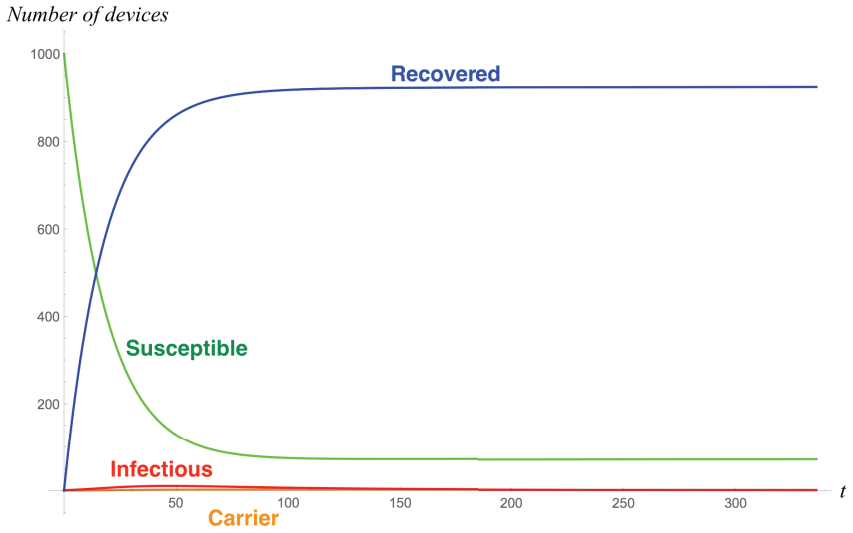

Figure 2: Evolution of the system to a disease-free steady state.

4. Design of efficient control measures

As is mentioned above, the basic reproductive number R_0 plays a very important role in the design of efficient control measures. Specifically, if $R_0 < 1$ the malware outbreak dies out and, consequently, the reduction of the numeric value of the R_0 will be the main goal of all control measures. In what follows, we will analyze the basic reproductive number in order to provide explicit expressions for the control of the malware epidemic.

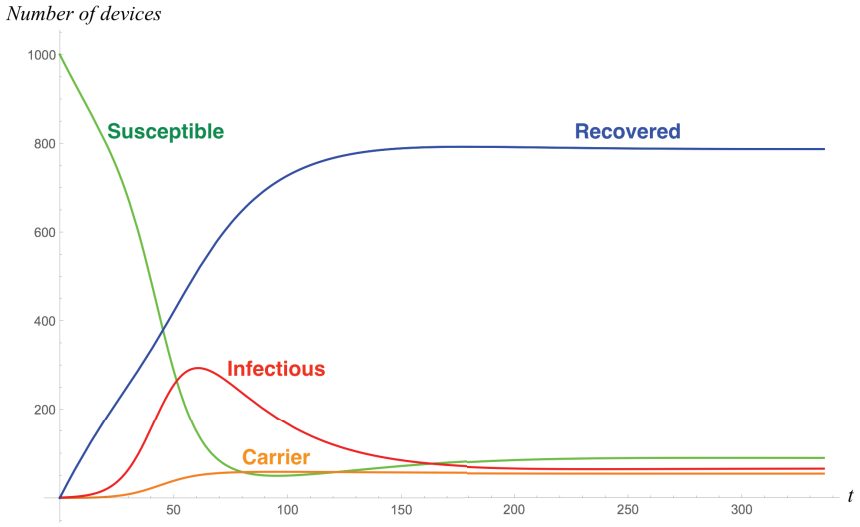

Figure 3: Evolution of the system to an endemic steady state.

4.1. One-parameter analysis

From the explicit expression of the basic reproductive number (26) and taking into account that $0 < a, b_I, b_C, \delta, v, \epsilon \leq 1$, we obtain the following:

$$\frac{\partial R_0}{\partial a} = \frac{N\epsilon\left(\left(1-\delta\right)b_I + b_C\delta\right)}{b_I b_C\left(v+\epsilon\right)} > 0, \tag{53}$$

$$\frac{\partial R_0}{\partial N} = \frac{a\epsilon\left(\left(1-\delta\right)b_I + b_C\delta\right)}{b_I b_C\left(v+\epsilon\right)} > 0, \tag{54}$$

$$\frac{\partial R_0}{\partial b_I} = -\frac{a\delta N\epsilon}{b_I^2\left(v+\epsilon\right)} < 0, \tag{55}$$

$$\frac{\partial R_0}{\partial b_C} = -\frac{a\left(1-\delta\right)N\epsilon}{b_C^2\left(v+\epsilon\right)} < 0, \tag{56}$$

$$\frac{\partial R_0}{\partial \delta} = \frac{aN\epsilon\left(b_C - b_I\right)}{b_I b_C\left(v+\epsilon\right)} \begin{cases} < 0, & \text{if } b_C < b_I \\ > 0, & \text{if } b_C > b_I \end{cases}, \tag{57}$$

$$\frac{\partial R_0}{\partial v} = -\frac{aN\epsilon\left(\left(1-\delta\right)b_I + b_C\delta\right)}{b_I b_C\left(v+\epsilon\right)^2} < 0, \tag{58}$$

$$\frac{\partial R_0}{\partial \epsilon} = \frac{aNv\left(\left(1-\delta\right)b_I + b_C\delta\right)}{b_I b_C\left(v+\epsilon\right)^2} > 0. \tag{59}$$

From these results we can obtain that R_0 decreases as a, N or ϵ decreases

(supposing that the rest of parameters remain constant). On the other hand, R_0 decreases as b_I, b_C and v increases (supposing that the rest of parameters remain constant). Furthermore, R_0 decreases if δ increases when $b_C < b_I$, or if δ decreases when $b_C > b_I$. As a consequence, in absence of additional measures, the following reduce the impact of the malware epidemic:

- Decreasing the transmission rate or the rate of lose of immunity by increasing the security knowledge and awareness of devices' users.
- Increasing the recovery rates and the vaccination rate by using efficient anti-virus software.

The rest of control measures obtained from the above implies the control of the population (decreasing the total number of devices N and increasing/decreasing the fraction of devices with a non-targeted operative system δ), and this is not realistic.

4.2. Two-parameter analysis

Now, we will study the basic reproductive number when all parameters remain constant with the exception of two. For the sake of simplicity we will study the pairs (v, a) and (v, ϵ).

If we suppose that all parameters remain constant with the exception of a and v, the R_0 can be understood as a function of two variables: $R_0 = R_0(a, v)$. Set $p = (v_0, a_0)$ the initial point in the va-plane such that it is placed in the endemic region defined $R_0 > 1$ (see Figure 4).

The optimal trajectory to the disease-free region is given by the line connecting the points p and $\bar{p}$ (which is perpendicular to the line $R_0 = 1$). A simple computations shows that:

$$\bar{p} = (\bar{v}, \bar{a}) = \left(\frac{a_0\alpha + \alpha^2 v_0 - \epsilon}{\alpha^2 + 1}, \frac{a_0 + \alpha(v_0 + \epsilon)}{\alpha^2 + 1} \right) = \left(\bar{v}, \frac{\bar{v} + \epsilon}{\alpha} \right), \tag{60}$$

where

$$\alpha = \epsilon N \frac{(1 - \delta) b_I + \delta b_C}{b_I b_C}. \tag{61}$$

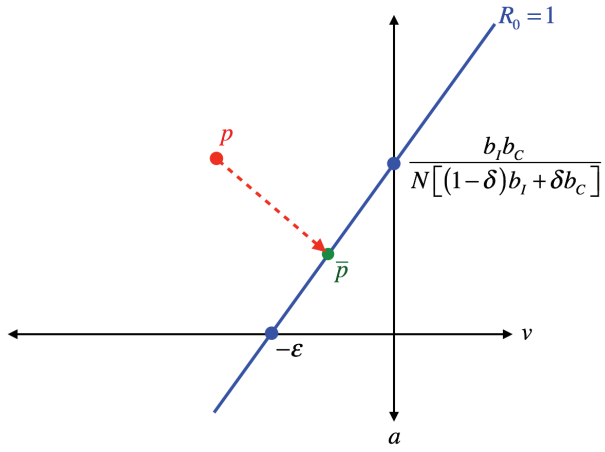

Figure 4: Graphic scheme for the optimization of control measures based on a and v.

As a consequence the best strategy to reduce R_0 modifying only the parameters a and v is to increase v and decrease a such that $a = \frac{v+\epsilon}{\alpha}$, for each value of the modified v.

Similarly, if $R_0 = R_0(v, \epsilon)$ and $p = (v_0, \epsilon_0)$ belongs to the endemic region, the nearest point to p of the straight line $R_0 = 1$ is given by:

$$\bar{p} = (\bar{v}, \bar{\epsilon}) = \left(\frac{(\alpha - 1)(\alpha v_0 - v_0 + \epsilon_0)}{\alpha^2 - 2\alpha + 2}, \frac{\alpha v_0 - v_0 + \epsilon_0}{\alpha^2 - 2\alpha + 2} \right) = \left(\bar{v}, \frac{\bar{v}}{\alpha - 1} \right), \quad (62)$$

where

$$\alpha = aN \frac{(1-\delta) b_I + \delta b_C}{b_I b_C}. \quad (63)$$

Consequently the better way to reduce R_0 considering only the parameters v and ϵ is to increase v and decrease ϵ such that $\epsilon = \frac{v}{\alpha - 1}$ for each value of the modified v.

5. Conclusions

In this work a novel mathematical model to simulate malware spreading has been introduced. It is a compartmental model where the new class of carrier devices is considered (apart from susceptible, infectious and recovered). This new compartment is constituted by those devices that can be reached by the malware but they cannot be damaged although they can act as transmission vectors. Consequently, the incidence of the model depends both on infectious and carrier devices.

This additional type plays an important role since the temporal immunity rate for carriers and the fraction of the total population that belongs to carrier compartment appear in the expression of the basic reproductive number R_0.

The model presented is global and deterministic and its dynamics is governed by means of a system of ordinary differential equations. As a consequence, the qualitative theory can be used to study the stability of the disease-free and the endemic equilibrium points. In this sense, it is shown that the disease-free steady state is locally and globally asymptotically stable if $R_0 < 1$. On the other hand, the local and global stability of the endemic equilibrium point not only depends on the numeric value of the R_0 (in fact, it is locally and globally asymptotically stable when $R_0 > 1$) but also on other two conditions involving the parameters of the system.

Finally, an analytical study of the basic reproductive number yields mathematical expressions for the efficient control measures depending on only one epidemic parameter and two epidemic parameters.

Acknowledgments

This work has been supported by Ministry of Economy and Competitiveness (Spain) and European FEDER Fund under projects TIN2014-55325-C2-2-R, and MTM2015-69138-REDT.

References

[1] Singh S, Sharma PK, Moon SY, Moon D, Park JH. A comprehensive study on APT attacks and countermeasures for future networks and communications: challenges and solutions. The Journal of Supercomputing 2016; 1–32. doi:10.1007/s11227-016-1850-4

[2] Winkler I, Treu Gomes A. Advanced Persistent Security. A cyberwarfare Approach to Implementing Adaptive Enterprise Protection, Detection and Reaction Strategies. Cambridge, MA: Singress, Elsevier Inc; 2017.

[3] Alaba FA, Othman M, Hashem IAT, Alotaibi F. Internet of Thing security: A survey. J Netw Comput Appl 2017; 88:10–28.

[4] Ashibani Y, Mahmoud QH. Cyber physical systems security: Analysis, challenges and solutions. Comput Secur 2017; 68:81–97.

[5] Lopez J, Alcaraz C, Rodriguez J, Roman R, Rubio JE. Protecting Industry 4.0 against Advanced Persistent Threats. European CIIP Newsletter 2017; 11:27-9.

[6] Thames L, Schaefer D. Cybersecurity for Industry 4.0. Analysis for Design and Manufacturing. Springer International Publishing AG; 2017.

[7] Damodaran A, Ci Troia F, Visaggio CA, Austin TH, Stamp M. A comparision of static, dynamic, and hybrid analysis for malware detection. J Comput Virol Hack Tech 2017; 13: 1–12.

[8] Peng S, Yu S, Yang A. Smartphone malware and its propagation modeling: A survey. IEEE Commun Surv Tut 2014; 16(2): 925–941.

[9] Martín-del Rey A. Mathematical modeling of the propagation of malware: A review. Secur Commun Netw 2015; 8(15): 2561-2579.

[10] Liu W., Liu C., Liu X., Cui S., Huang X. Modeling the spread of malware with the influence of heterogeneous immunization. Appl Math Model 2016; 40(4): 3141–3152.

[11] Abazari F, Analoui M, Takabi H. Effect of anti-malware software on infectious nodes in cloud environment. Comput Secur 2016; 58: 139–148.

[12] Dong T, Wang A, Liao X. Impact of discontinuos antivirus strategy in a computer virus model with the point to group. Appl Math Model 2016; 40(4):3400-3409.

[13] Hernández-Guillén JD, Martín-del Rey A, Hernández Encinas L. Study of the stability of a SEIRS model for computer worm propagation. Physica A 2017; 479: 411–421.

[14] Hosseini S, Azgomi MA, Rahmani AT. Malware propagation modeling considering software diversity and inmunization. J Comput Sci 2016; 13: 49–67.

[15] Liu W, Zhong S. Web malware spread modelling and optimal control strategies. Sci Rep 2017; 7: 42308.

[16] Upadhyay RK, Kumari S, Misra AK. Modeling the virus dynamics in computer network with SVEIR model and nonlinear incident rate. J Appl Math Comput 2017; 54(1): 485–509.

[17] Wang F, Huang W, Shen Y, Wang C. Analysis of SVEIR worm attack model with saturated incidence and partial immunization. J Commun Info Netw 2016; 1(4): 105-115.

[18] Bonyah E, Atangana A, Khan MA. Modeling the spread of computer virus via Caputo fractional derivative and the beta-derivative. Asia Pac J Comput Engin 2017; 4: 1. DOI 10.1186/s40540-016-0019-1.

[19] Zhang ZZ, Bi DJ. Dynamical analysis of a computer virus propagation model with delay and infectivity in latent period. Discrete Dyn Nat Soc 2016; 2016: Article ID 3067872. http://dx.doi.org/10.1155/2016/3067872.

[20] Hosseini S, Azgomi MA, Torkaman AR. Agent-based simulation of the dynamics of malware propagation in scale-free networks. Simul-Trans Soc Model Simul Int 2016; 92(7): 709-722.

[21] Pu C, Li S, Yang X, Xu Z, Ji Z, Yang J. Traffic-driven SIR epidemic spreading in networks. Physica A 2016; 446: 129–137.

[22] Ren J, Liu J Xu Y. Modeling the dynamics of a network-based model of virus attacks on targeted resources. Commun Nonlinear Sci Numer Simul 2016; 31: 1–10.

[23] Amador J. The SEIQS stochastic epidemic model with external source of infection. Appl Math Model 2016; 40: 8352–8365.

[24] Yorke JA. Invariance for ordinary differential equations. Math Syst Theory. 1967; 1(4): 353–372.

[25] Wiggins S. Introduction to applied nonlinear dynamical systems and chaos, vol 2. New York: Springer Verlag; 2003.

[26] Diekmann O, Heesterbeek H, Britton T. Mathematical Tools for Understanding Infectious Disease Dynamics. Princeton: Princeton University Press; 2013.

[27] van den Diressche P, Watmough J. Further Notes on the Basic Reproduction Number. In: Brauer F, van den Driessche P, Wu J, editors. Mathematical Epidemiology, Berlin: Springer-Verlag; 2008, p. 159–178.

[28] Merkin DR. Introduction to the Theory of the Stability, vol 24. New York: Springer-Verlag, 2012.

[29] La Salle JP. The stability of dynamical systems. SIAM, 1976.

[30] McNabb A. Comparision theorems for differential equations. J Math Anal Appl 1986; 119: 417–428.

[31] Freedman H, Ruan S, Tang M. Uniform persistence and flows near a closed positively invariant set. J Dyn Differ Eq 1994; 6(4): 583–600.

[32] Hutson V, Schmitt K. Permanence and the dynamics of biological systems. Math Biosci 1992; 111(1): 1–71.

[33] Martin RH. Logarithmic norms and projections applied to linear differential systems. J Math Anal Appl 1974; 45(2): 432–454.

[34] Buonomo B, Lacitignola D. Analysis of a tuberculosis model with a case study in Uganda. J Biol Dyn 2010; 4(6): 571–593.

[35] Zhu Q, Yang X, Ren J. Modeling and analysis of the spread of computer virus. Commun Nonlinear Sci Numer Simul 2012; 17(12): 5117–5124.

[36] Li MY, Muldowney JS. A geometric approach to global-stability problems. SIAM J Math Anal 1996; 27(4): 1070–1083.