



CAN UNCLASSIFIED



DRDC | RDDC  
technologysciencetechnologie

# Modelling cyber vulnerability using epidemic models

Bao Nguyen

DRDC – Centre for Operational Research and Analysis

**Defence Research and Development Canada**

Scientific Report

DRDC-RDDC-2017-R213

May 2018

CAN UNCLASSIFIED





## IMPORTANT INFORMATIVE STATEMENTS

**Disclaimer:** Her Majesty the Queen in right of Canada, as represented by the Minister of National Defence ("Canada"), makes no representations or warranties, express or implied, of any kind whatsoever, and assumes no liability for the accuracy, reliability, completeness, currency or usefulness of any information, product, process or material included in this document. Nothing in this document should be interpreted as an endorsement for the specific use of any tool, technique or process examined in it. Any reliance on, or use of, any information, product, process or material included in this document is at the sole risk of the person so using it or relying on it. Canada does not assume any liability in respect of any damages or losses arising out of or in connection with the use of, or reliance on, any information, product, process or material included in this document.

This document was reviewed for Controlled Goods by Defence Research and Development Canada (DRDC) using the Schedule to the *Defence Production Act*.

**Endorsement statement:** This publication has been peer-reviewed and published by the Editorial Office of Defence Research and Development Canada, an agency of the Department of National Defence of Canada. Inquiries can be sent to:  
[Publications.DRDC-RDDC@drdc-rddc.gc.ca](mailto:Publications.DRDC-RDDC@drdc-rddc.gc.ca).



## Abstract

---

This Scientific Report (SR) documents an epidemic model known as SIR (Susceptible-Infected-Removed units). We derive an approximated solution to the differential equations that define the SIR model. Unlike the exact SIR solution, the approximate solution is analytical and has a close form expression. We use this approximate model as an inspiration to cyber defence. Such a model allows us to investigate the characteristics of the propagation of electronic viruses. That is, we can determine the number of susceptible units, the number of infected unit and the number of removed units as a function of time. This information will eventually permit the defence to find ways to eradicate a virus attack.

## Significance to defence and security

---

Biological diseases have been known to man since time immemorial. Nowadays, we also encounter electronic viruses. Since we live in an electronic world, electronic viruses cause billions of dollars of damage each year, Ref [1], in addition to security breaches and loss of confidential information. If a virus attacks a task group, it can make the defence fire in the wrong direction, at the wrong time and at the wrong target. So it is important that we understand how virus propagates in a network that is under attack.

We are inspired by an epidemic model known as the SIR (Susceptible-Infected-Removed) model defined by a set of differential equations. The SIR model allows us to determine the number of susceptible units that can be infected, the number of infected units that can spread infections and the number of removed units (those recovered from infection). The current SIR model has no known analytical solutions and hence requires numerical solutions which make it inconvenient to study the SIR units as a function of time especially if the parameters that define the SIR differential equations vary from one defence system to another or vary with time within the same system. However, we derive an approximate (new) model of SIR which has an analytical solution and all the features of the original SIR model.

The new model is a tool that can be used to plan for an electronic virus attack and find ways to defend against such an attack. That is, we can determine the number of units such as computers or defence system components that are infected and how long the infection lasts. Eventually, this will affect the defence effectiveness especially against an astute enemy that launches simultaneously a missile attack as well as a cyber-attack against a task group for example. If the command and control system is infected, key measures of effectiveness such as the probability of raid annihilation is expected to be affected.

The scientific contribution to this report is the operational research modelling of a virus propagation. The model that we analyze contains all the essential elements of a generic virus propagation yet at the same time does not involve detailed aspects of specific virus infections which makes it an ideal operational research tool to investigate the time scale of an infection and its remedy. We are able to derive an approximate solution that is analytical and therefore very useful in defence planning. The novelty of the solution lies in the concavity and the simplicity of the functional approximation of the differential equations both of which are not known in the open literature to the best of our knowledge.



## Résumé

---

Ce rapport scientifique fait état d'un modèle épidémique appelé SIR (Sensible-Infecté-Retiré). Nous obtenons une solution approximative aux équations différentielles qui définissent le modèle SIR. Contrairement à la solution SIR exacte, la solution approximative est analytique et elle a une expression en forme fermée. Nous utilisons ce modèle approximatif comme inspiration pour la cybersécurité. Un tel modèle nous permet d'étudier les caractéristiques de la propagation de virus électroniques. C'est-à-dire que nous pouvons déterminer le nombre d'unités sensibles, le nombre d'unités infectées et le nombre d'unités retirées en fonction du temps. Cette information permettra ensuite à la défense de trouver des façons d'éradiquer une attaque virale.

## Importance pour la défense et la sécurité

---

L'être humain connaît les maladies biologiques depuis la nuit des temps. De nos jours, nous sommes également confrontés à des virus électroniques. Étant donné que nous vivons dans un monde électronique, les virus électroniques causent des milliards de dollars de dommages chaque année, Réf. [1], en plus des atteintes à la sécurité et de la perte de renseignements confidentiels. Si un virus attaque un groupe opérationnel, il peut inciter la défense à tirer dans la mauvaise direction, au mauvais moment ou sur la mauvaise cible. Il est donc important que nous comprenions comment les virus se propagent dans un réseau qui subit une attaque.

Nous avons été inspirés par un modèle épidémique appelé SIR (Sensible-Infecté-Retiré), défini par un ensemble d'équations différentielles. Le modèle SIR nous permet de déterminer le nombre d'unités sensibles qui pourraient être infectées, le nombre d'unités infectées qui peuvent répandre les infections et le nombre d'unités retirées (celles qui ne sont plus infectées). Le modèle SIR actuel ne comprend aucune solution analytique et, par conséquent, il exige des solutions numériques, ce qui le rend inapproprié pour l'étude des unités SIR en fonction du temps, surtout si les paramètres qui définissent les équations différentielles SIR varient d'un système de défense à un autre ou varient avec le temps dans un même système. Cependant, nous pouvons dériver un (nouveau) modèle SIR approximatif qui a une solution analytique et toutes les caractéristiques du modèle SIR original.

Le nouveau modèle est un outil pouvant être utilisé pour se prémunir contre une attaque par un virus électronique et trouver des façons de se défendre contre une telle attaque. C'est-à-dire, nous pouvons déterminer le nombre d'unités (ordinateurs ou composants d'un système de défense) qui sont infectées, ainsi que la durée de l'infection. En fin de compte, cela aura une incidence sur l'efficacité de la défense, surtout contre un ennemi astucieux qui, par exemple, lancerait simultanément une attaque par missiles et une cyberattaque contre un groupe de défense. Si le système de commandement et de contrôle est infecté, on s'attend à ce que des mesures essentielles de l'efficacité soient touchées, comme la probabilité d'anéantissement des raids.

La contribution scientifique à ce rapport est la modélisation de recherche opérationnelle de la propagation d'un virus. Le modèle que nous analysons contient tous les éléments essentiels d'une propagation générique d'un virus, mais sans tenir compte des aspects détaillés d'infections par un virus particulier, ce qui en fait un outil de recherche opérationnelle idéal pour étudier l'échelle de temps d'une infection et de son remède. Nous sommes en mesure de dériver une solution approximative qui est analytique et, par conséquent, très utile dans la planification de la défense. La nouveauté de la solution se trouve dans la concavité et la simplicité de l'approximation fonctionnelle des équations différentielles, deux éléments qui, au meilleur de nos connaissances, ne se trouvent nulle part dans la documentation libre d'accès.



## Table of contents

---

Abstract . . . . .	i
Significance to defence and security . . . . .	i
Résumé . . . . .	ii
Importance pour la défense et la sécurité . . . . .	ii
Table of contents . . . . .	iii
List of figures . . . . .	iv
Acknowledgements . . . . .	v
1 Introduction . . . . .	1
2 SIR Model of Epidemics . . . . .	4
3 Approximated Differential Equations to the SIR Epidemic Model . . . . .	6
4 Approximated Solution to the SIR Epidemic Model . . . . .	12
5 Results . . . . .	14
6 Properties of the Approximated Solution . . . . .	18
6.1 Number of infected units . . . . .	18
6.2 Limits as $t \rightarrow \infty$ . . . . .	19
6.3 Further corrections. . . . .	19
7 Conclusion . . . . .	22
References . . . . .	23
List of symbols/abbreviations/acronyms/initialisms . . . . .	26



## List of figures

---

Figure 1:	An SIR model. . . . .	4
Figure 2:	Lambert function.. . . .	8
Figure 3:	Derivative of $f$ . . . . .	11
Figure 4:	Number of infected units as a function of time. . . . .	14
Figure 5:	Number of susceptible units as a function of time.. . . .	15
Figure 6:	Number of removed units as a function of time.. . . .	15
Figure 7:	Number of susceptible, infected and removed units as a function of time. . . . .	16
Figure 8:	Number of susceptible, infected and removed units as a function of time. . . . .	16



---

## Acknowledgements

---

I would like to thank Prof. Suruz Miah of Bradley University and Dr. Kevin Ng of DRDC – Centre for Operational Research and Analysis for discussions.



This page intentionally left blank.



# 1 Introduction

---

“Infectious diseases have been a part of the human condition since time immemorial” Ref [2]. Nowadays, we also encounter electronic viruses which can attack computers and networks. The nature of data communication allows electronic viruses to propagate data rates ranging from kilobits per second to gigabits per second. Hence a network could be infected in a matter of minutes. To prepare defence against viruses, we need to be able to model the process of infection. Our inspiration is owed to the modelling of epidemiology.

Ref [2]: “Mathematical epidemiology has its roots in 1760, when Daniel Bernoulli formulated and solved a model for smallpox. In 1906, Hamer used a discrete-time model of measles to understand recurrent epidemics.” Clearly, there is an available body of knowledge in the mathematics of infectious diseases.

We encounter computer viruses and hackings every day and very much in every field of work. There are lots of speculations on the potential damages of a cyber-attack. Below is a list of examples:

- a. A car’s accelerator can be disabled, Ref [3];
- b. A car can unintended accelerate, brake or steer, Ref [4];
- c. A sniper rifle can be deactivated or change its target, Ref [5]; and
- d. The fact that North Korea’s missile launches were failing too often may be due to US cyber-attacks, Ref [6].

Some of the above examples may be real and some of them may be purely hypothetical and even false. But whatever their veracities are, cyber defence is real. It was even mentioned in the presidential debate between Hilary Clinton and Donald Trump, Ref [7]. It is not hard to imagine what would happen if a weapon system is infected. For example, the weapon system can fire in the wrong direction, at the wrong target and at the wrong time.

The economic impact of crimes in cyberspace is also speculated. Below are two examples.

- a. The cost of crimes in cyberspace is estimated to be 445 billion USD, Ref [8]; and
- b. US, China and Germany, three of the four largest economies in the world, lost more than 200 billion USD, Ref [9].

In addition to the extent of a cyber-attack, it is common knowledge that such an attack does not necessarily require a lot of resources as cited from Ref [10] below:

Cyberattacks are not resource-intensive, which renders them even more dangerous because no practical requirement exists to limit the attackers to being members of organized and well-funded sources such as a nation’s military.

This is also recognized officially by NATO as cited from Ref [11] below:

Cyber threats and attacks are becoming more common, sophisticated and damaging. The Alliance (NATO) is faced with an evolving complex threat environment. State and non-state actors can use cyber-attacks in the context of military operations.

Given the currency and extent of cyberattacks, we investigate the infection of viruses on a network using an epidemic model. It is certainly not the first time that cybersecurity is modelled by epidemiology, Refs [12][13]. There are several such models. To name a few: the SEIR model (Susceptible-Exposed-Infected-Removed), the SIR model (Susceptible-Infected-Removed), the SI model (Susceptible-Infectious) and the SIS model (Susceptible-Infectious-Susceptible), Ref [14].

The difference between the first two, the SEIR model and the SIR model, is that the former simulates the exposed phase where an individual can be infected but is not infectious, Ref [15]. It is often possible to neglect the exposed phase which leads to the SIR model, Ref [14] where an individual can be susceptible, infected or recovered. Susceptible units are those that can be infected. Infected units are those that can infect other units. And Removed units are those that are no longer infected (recovered units).

In contrast to the SIR model, the SI model does not account for the recovered phase. The SI model is usually appropriate for plants. Once the plants are infectious, they will remain infectious and eventually die, Ref [14]. The remaining model, i.e. the SIS model, is appropriate for sexually transmitted diseases. Once an individual recovers, he/she is again susceptible to infection, Ref [14].

Based on the nature of the cyber defence scenarios that we consider: suitability of the level of details, rapid dissemination of the infection (time scale is short, Ref [16]) and the fact that a recovered unit is not susceptible to infection once the virus is known and there is a software that can neutralize the virus, we choose to examine the SIR model as a cyber defence model.

Similar to most of the epidemic models, the SIR model does not have analytical solutions. Hence, it only has numerical solutions which make it inconvenient (but not impossible) to analyze and to predict the extent of the infection. However, we were able to find an approximate solution that is analytical. And we will show in future work that the approximated SIR model is useful in planning against cyberattacks.

Section 2 presents a SIR model. Section 3 derives an approximated differential equation to the SIR model. Section 4 derives an approximated solution which is a solution to the approximated differential equation. Section 5 analyzes the results. Section 6 provides the characteristics of the approximated solution. We conclude in Section 7.

This report draws extensively from Ref [17]. The significance to defence and security statement of this report is original. Section 6 of this report contains original material that is not in Ref [17] except for the long term results to the SIR model. Discussion of the numerical results regarding the use of look up tables is also original. Conclusion is also substantiated. Generally, there are more details in this report as well as the fact that interpretations to military applications are made obvious.

Before we delve into the details of the report, we state below the assumptions:

- a. It is possible for a red force to hack into the defence system and put a virus in the defence system;
- b. The defence is partially disabled if not completely during the infection;

- c. The nature of cyber vulnerabilities may be simulated by biological epidemic models (Refs [18][19]) but with a different time scale; and
- d. Further studies/experiments can refute the model and/or determine the parameters of the epidemic models.

Note that the epidemic models described above are simple and deterministic. There are also stochastic models (Ref [20]) but they are even more complicated mathematically and are not necessarily better for our purpose than the SIR model. In fact, there are a multitude of computer viruses such as benevolent viruses, file infectors, macro viruses, etc. (Ref [21]). Each of them behaves differently. It would be impossible to model all of them.

We are well aware that there is definitely a difference between computer viruses and biological viruses, Ref [22]. But that does not mean epidemic models are not useful in modelling cyber defence. For example, Refs [18][19] make use differential equations that are similar to epidemic models to examine cyber vulnerabilities.

Ultimately, we aim to determine the effects of a cyber-attack on the effectiveness of the defence and not the details of the infection in the sense that we are looking for orders of magnitudes for the number of susceptible units, the number of infected units and the number of removed units as well as the duration of the infection. In essence, if there is a virus in the system and if there is a remedy to that virus and both of them can be modelled or bound by the parameters in the SIR model then the solution to the SIR model can be useful to the planning of cyber defence. This solution will enable the comparison the efficiency between cyber defence software against known viruses. Knowing the magnitudes of the duration of the infection and the magnitudes of the number of components that are affected will help determine the changes in defence effectiveness. This is critical especially against an astute enemy who could launch a missile attack at the same time as a cyber-attack. It is not hard to imagine how things can go wrong to a net centric defence when the command and control is infected even if for a short time. Key measures of effectiveness such as the probability of raid annihilation will definitely be affected.

## 2 SIR Model of Epidemics

---

The SIR model is well understood, Ref [2]. It is assumed in the SIR model that the population is homogeneous. That is, each type of unit has the same behaviour. For example, each \*healthy\* unit has the same rate of infection. Such homogeneity is easy to model mathematically as shown in Eqn (1). In reality, there is no reason for a population or a network to be homogeneous. Such a population can be broken down into smaller groups each having its own characteristics. In terms of connectivity, homogeneity can occur when any unit is in contact with any other units, Ref [23]. This interpretation can be seen when we consider a finite population for example four units in which one of them is infected. If the infection rate is the same for all susceptible units then all units must be in contact with all other units. Otherwise, by changing the initial infected unit to another unit, we will not have the same infection rate. This corresponds to a complete graph (Ref [24]) which is a graph where every node is linked to any other nodes. In other words, this is a totally connected network. Clearly, the spread of a virus depends on the topology of the network, Refs [25][26]. That is, infections could occur only if an infected node is connected to another node. Therefore, we can consider the SIR model as the worst case scenario, i.e. an infected node can infect any other nodes. We could also think of the SIR model as an attack at the central node which is connected to all of the other nodes: something an astute enemy would do. It is defined by a set of differential equations as shown below:

$$\begin{aligned}\frac{dS}{dt} &= -aSI \\ \frac{dI}{dt} &= aSI - bI \\ \frac{dR}{dt} &= bI\end{aligned}\tag{1}$$

where  $S$  is the number of units that are susceptible to infections,  $I$  is the number of units infected and  $R$  is the number of units removed from infection, i.e. they are no longer infected;  $a$  is the rate of infection and  $b$  is the rate of recovery (Figure 1).  $N = S + I + R$  is a constant in the SIR model. That is, the total population is fixed. We scale  $S' = S/N$ ,  $I' = I/N$  and  $R' = R/N$ . Hence,  $0 \leq S', I', R' \leq 1$  and  $(S/N) + (I/N) + (R/N) = N/N = 1$ . For convenience, we use  $S$  for  $S'$ , etc. In the context of computer viruses,  $S$  is the number of susceptible units,  $I$  is the number of infected units and  $R$  is the number of removed (recovered) units.



Figure 1: An SIR model.

In spite of the simplicity of Equation (1), there are no known analytical solutions. However, we could infer from Equation (1) that there are two equilibrium points where the RHS of Equation (1) are equal to zeroes. The first equilibrium point occurs when  $I = \bar{I} = 0$ ,  $S = \bar{S} \leq N$  and  $R = \bar{R} = N - \bar{S}$ . The second equilibrium occurs when  $aS - b = 0$  or  $S = \bar{S} = b/a$  which implies that  $dI/dt = 0$  which makes  $I = \bar{I} \leq N$  but  $S$  is decreasing due to  $dS/dt$ . Therefore it is not a stable equilibrium.

If  $S_0$  is the initial value of  $S$  at time zero and  $S_0 > b/a$  then there will be an epidemic as  $dI/dt > 0$ .

### 3 Approximated Differential Equations to the SIR Epidemic Model

---

We note that from Equation (1),  $R$  is uniquely determined by  $I$ . So we focus on  $S$  and  $I$  because once we solve for  $S$  and  $I$ , we can readily solve for  $R$ . The first two equations of Equation (1) can be combined to give:

$$\frac{dI}{dt} = -\frac{dS}{dt} - bI \quad (2)$$

We define

$$f(t) = \int_0^t I(t) dt \geq 0 \quad (3)$$

Integrating Equation (2), we get:

$$S = -I - b \cdot f + C \quad (4)$$

where  $C$  is a constant of integration. Since

$$\frac{1}{S} \frac{dS}{dt} = \frac{d \ln S}{dt} = -aI \quad (5)$$

We get

$$S = -\frac{df}{dt} - bf + C = Ae^{-af} \quad (6)$$

where  $A$  is a constant parameter. If we assume that there is  $I_0$  infection at time zero and there are no removed units then these are the boundary conditions:

$$\begin{aligned}
f(0) &= \int_0^0 I(t) dt = 0 \\
\frac{df}{dt} &= I(0) = I_0 \\
S(0) &= S_0 \\
S_0 + I_0 &= 1 \\
R_0 &= 0
\end{aligned} \tag{7}$$

This means that

$$\begin{aligned}
A &= S_0 \\
C &= 1
\end{aligned} \tag{8}$$

Hence,

$$\frac{df}{dt} = 1 - bf - S_0 e^{-af} \tag{9}$$

There are two roots to the RHS of Equation (9):

$$\begin{aligned}
f = f_1 &= \frac{1}{b} + \frac{1}{a} W \left( -1, \frac{-aS_0}{b} e^{-a/b} \right) \\
f = f_2 &= \frac{1}{b} + \frac{1}{a} W \left( 0, \frac{-aS_0}{b} e^{-a/b} \right)
\end{aligned} \tag{10}$$

where  $W$  is the Lambert function. Lambert function is shown in Figure 2. For real  $x$ , there are two branches. The first branch is shown in blue and corresponds to  $W(0, x)$  while the second branch is shown in yellow and corresponds to  $W(-1, x)$ .

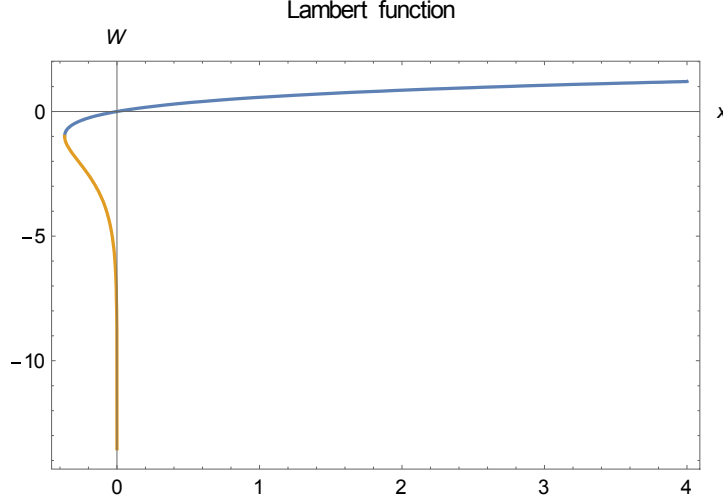


Figure 2: Lambert function.

Since the arguments of  $W(x)$  for  $f_1$  and  $f_2$  are negative, we can infer that the  $Ws$  embedded in  $f_1$  and  $f_2$  are also negative based on Figure 2. Simple calculus dictates that  $-S_0 u e^{-u} \geq -S_0 / e$  where  $u = a / b$ . From Equation (1), there are two cases. First, if  $a < b$  ( $u < 1$ ) then the number of infected units will decrease right away. That is, the infection will die out with time. Second, if  $a \geq b$  ( $u \geq 1$ ) then the number of infected units will increase at least at time zero. Therefore, we will focus on the second case because the virus will infect the system which is the scenario that we are interested in. Since  $S_0 \leq 1$ , we reason that:

$$W(0, -S_0 u e^{-u}) = -\lambda \geq -1 \quad (11)$$

Hence

$$f = f_2 = \frac{1}{b} + \frac{1}{a} W\left(0, \frac{-aS_0}{b} e^{-a/b}\right) = \frac{a - \lambda b}{ab} = \frac{u - \lambda}{bu} \geq 0 \quad (12)$$

From Ref [27], the second order approximation of  $W(-1, x)$  is given by:

$$W(-1, -e^{-1-z^2/2}) \approx -1 - z \quad (13)$$

Equating



$$e^{-1-z^2/1} = S_0 u e^{-u} \quad (14)$$

We obtain:

$$z = \sqrt{-2(\ln S_0 + \ln u - u + 1)} \quad (15)$$

If  $S_0 \approx 1$  then by using a Taylor expansion, we get

$$z = u - 1 + \frac{(u-1)^2}{3} + O((u-1)^3) \quad (16)$$

As a result

$$W(-1, -e^{-1-z^2/2}) \approx -u - (u-1)^2/3 \quad (17)$$

Hence

$$f = f_1 = \frac{1}{b} + \frac{1}{a} W\left(-1, \frac{-aS_0}{b} e^{-a/b}\right) = -\frac{(u-1)^2}{3a} < 0 \quad (18)$$

The above holds in general for  $0 < S_0 \leq 1$ .

We observe that the RHS of Equation (9) is concave. That is,

$$RHS\left(\frac{x+y}{2}\right) \geq \frac{1}{2}(RHS(x) + RHS(y)) \quad (19)$$

Equivalently,

$$\begin{aligned}
1 - b \frac{(x+y)}{2} - S_0 e^{-a \frac{(x+y)}{2}} &\stackrel{?}{\geq} \frac{1}{2} \left\{ (1 - bx - S_0 e^{-ax}) + (1 - by - S_0 e^{-ay}) \right\} \\
-e^{-a \frac{(x+y)}{2}} &\stackrel{?}{\geq} -\frac{1}{2} (e^{-ax} + e^{-ay}) \\
0 &\stackrel{?}{\leq} \frac{1}{2} \left( e^{-ax} - 2e^{-a \frac{(x+y)}{2}} + e^{-ay} \right) \\
0 &\leq \left( e^{-ax/2} - e^{-ay/2} \right)^2
\end{aligned} \tag{20}$$

Because the RHS of Equation (9) is concave, we approximate it by a quadratic function. That is,

$$1 - bf - e^{-af} \approx c(f - f_1)(f - f_2) \tag{21}$$

where  $f_1$  and  $f_2$  are given by Equation (10). Additionally, we determine  $c$  by minimizing the  $\chi^2$ , i.e.

$$\min_c \int_0^{f_2} df \cdot \left\{ c \cdot (f - f_1) \cdot (f - f_2) - (-b \cdot f - e^{-af} + 1) \right\}^2 \tag{22}$$

which is the same as

$$\begin{aligned}
\frac{d}{dc} \int_0^{f_2} df \left\{ c(f - f_1)(f - f_2) - (-bf - S_0 e^{-af} + 1) \right\}^2 &= 0 \\
\int_0^{f_2} df \left\{ c(f - f_1)(f - f_2) - (-bf - S_0 e^{-af} + 1) \right\} (f - f_1)(f - f_2) &= 0 \\
\int_0^{f_2} df \left\{ c(f - f_1)^2 (f - f_2)^2 - (f - f_1)(f - f_2)(-bf - S_0 e^{-af} + 1) \right\} &= 0
\end{aligned} \tag{23}$$

This yields:

$$c = \frac{\int_0^{f_2} df \left\{ (f - f_1)(f - f_2)(-bf - S_0 e^{-af} + 1) \right\}}{\int_0^{f_2} df \left\{ (f - f_1)^2 (f - f_2)^2 \right\}} \tag{24}$$

There is actually a close form expression for  $c$ . It can be obtained by performing the integrals in the numerator and in the denominator above. However, it is not particularly illuminating so we keep Equation (24) the way it is. Observe that the integrals in Equation (24) are integrated from  $f = 0$  to  $f = f_2 > 0$  since we know that  $f(t) \geq 0$  as shown in Equation (3). By doing so, we discard all negative values of  $f$  which are not physical values. That is, the value of  $c$  is not affected by the value of  $f$  when  $f$  is negative.

We plot the exact  $\frac{df}{dt}$  in Equation (9) and the quadratic function in Equation (21) that approximates  $\frac{df}{dt}$  in Figure 3. It can be seen that the approximation is very similar to the exact  $\frac{df}{dt}$ . Both of them are concave functions with a maximum between  $f_1$  and  $f_2$ .

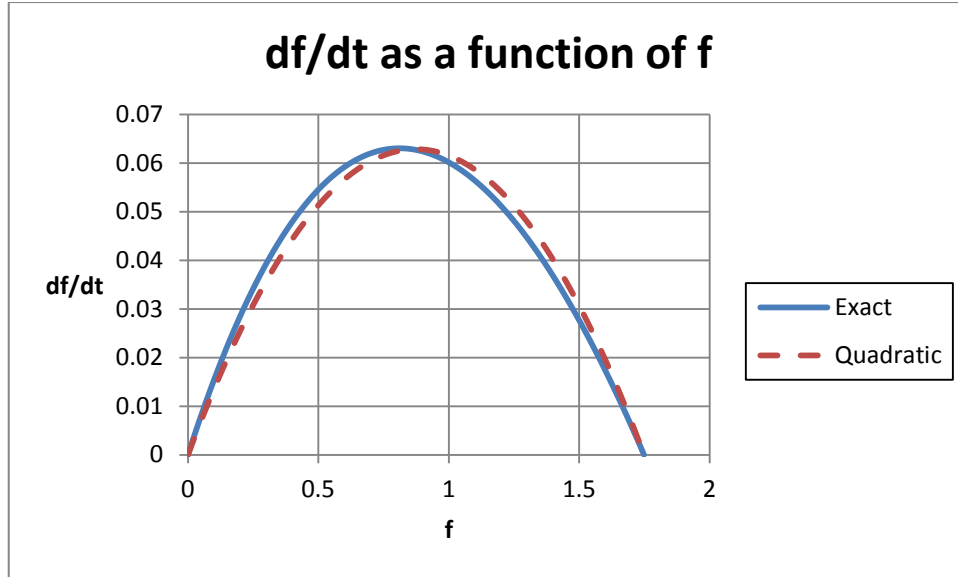


Figure 3: Derivative of  $f$ .

For illustration, we assume the following values in Figure 3:

$$\begin{aligned}
 a &= 1/2 \\
 b &= 1/3 \\
 S_0 &= 0.99999 \\
 f_1 &= -5.99991 \cdot 10^{-5} \\
 f_2 &= 1.74847
 \end{aligned} \tag{25}$$

Note that the above approximation was also reported in Ref [17].

## 4 Approximated Solution to the SIR Epidemic Model

---

We now solve for  $f(t)$  using the quadratic approximation:

$$\frac{df}{dt} = c(f - f_1)(f - f_2) \quad (26)$$

This is a simple differential equation that can be solved using:

$$\frac{df}{c(f - f_1)(f - f_2)} = dt \quad (27)$$

Ref [28], Integrating:

$$\frac{1}{\sqrt{\Delta}} \ln \left( \frac{f - f_1}{f_2 - f} \right) = t + C \quad (28)$$

where  $C$  is a constant parameter and  $\sqrt{\Delta} = c(f_1 - f_2) > 0$  assuming that  $c < 0$ ,  $f_1 < 0$  and  $f_2 > 0$ . Raising Equation (28) as a power of an exponential, we get:

$$\frac{f - f_1}{f_2 - f} = A \cdot e^{\sqrt{\Delta}t} \quad (29)$$

where  $A$  is a constant parameter. Since  $f(0) = 0$ , this yields:

$$A = -\frac{f_1}{f_2} \quad (30)$$

Solving for  $f$ :

$$f = \frac{f_2(-1 + e^{\sqrt{\Delta}t})}{-f_2/f_1 + e^{\sqrt{\Delta}t}} \quad (31)$$

We can now obtain  $I(t)$ :

$$I(t) = \frac{d}{dt} f(t) = \frac{cf_1f_2e^{\sqrt{\Delta}t} (f_1 - f_2)^2}{(f_2 - f_1e^{\sqrt{\Delta}t})^2} \quad (32)$$

From Equation (5) and the boundary conditions in Equation (7), we get an expression for  $S(t)$ :

$$S(t) = S_0 e^{-af(t)} \quad (33)$$

From Equation (1) and the boundary conditions in Equation (7), we get an expression for  $R(t)$ :

$$R(t) = bf(t) \quad (34)$$

Note that the above solution was also reported in Ref [17].

## 5 Results

We plot  $I$  as a function  $t$  in Figure 4.  $I$  increases as a function of time then reaches a maximum and then decreases as a function of time. The blue curve corresponds to the exact solution obtained numerically while the red curve corresponds to the approximated solution. The two have the same shape and the same asymptotic behaviours as time gets large. In addition, the approximated solution is slightly shifted to the right. The maximum number of infected units is about 6.2 percent of the population as  $I$  is normalized. The input parameters are shown in Equation (25). Note that we did not give a unit for the time as we do not know the coupling parameters  $a$  and  $b$ . Once we obtain the values for the coupling parameters, we will be able to extract the unit of time. This will be done in the future.

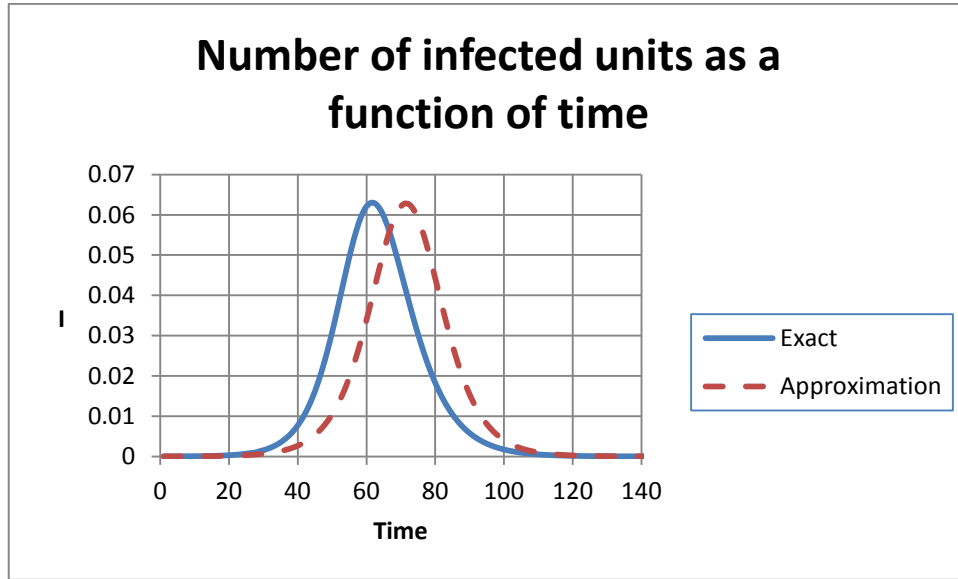


Figure 4: Number of infected units as a function of time.

Similarly, we plot  $S$  as a function of  $t$  in Figure 5. It is a decreasing function of time. The blue curve corresponds to the exact solution while the red curve corresponds to the approximated solution. The two have the same shape and the same asymptotic behaviours as time gets large. That is,  $S$  reaches constant value that is not zero for large time. In addition, the approximated solution is slightly shifted to the right.

The same behaviours occur when we plot  $R$  as a function of  $t$  as shown in Figure 6. It is an increasing function of time and reaches a non-zero value as time gets large. We plot the SIR units as a function of time for the exact model in Figure 7 and for the approximate model in Figure 8. As time gets large, the SIR units in both cases reach steady values.

### Number of susceptible units as a function of time

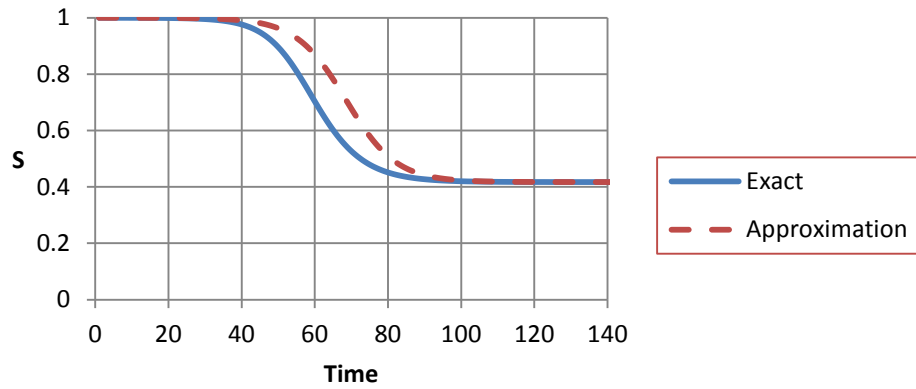


Figure 5: Number of susceptible units as a function of time.

### Number of removed units as a function of time

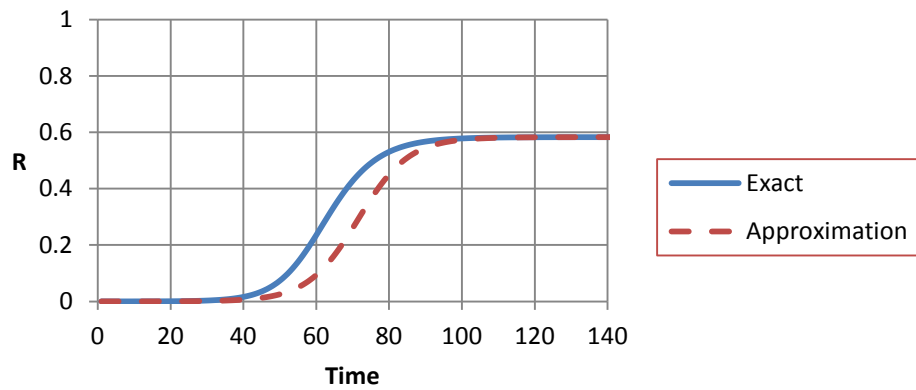


Figure 6: Number of removed units as a function of time.

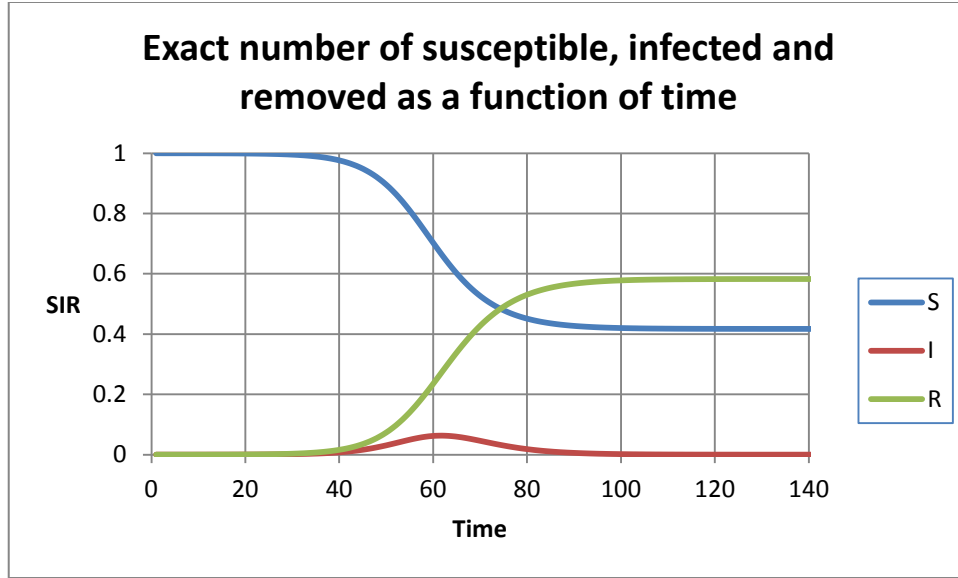


Figure 7: Number of susceptible, infected and removed units as a function of time.

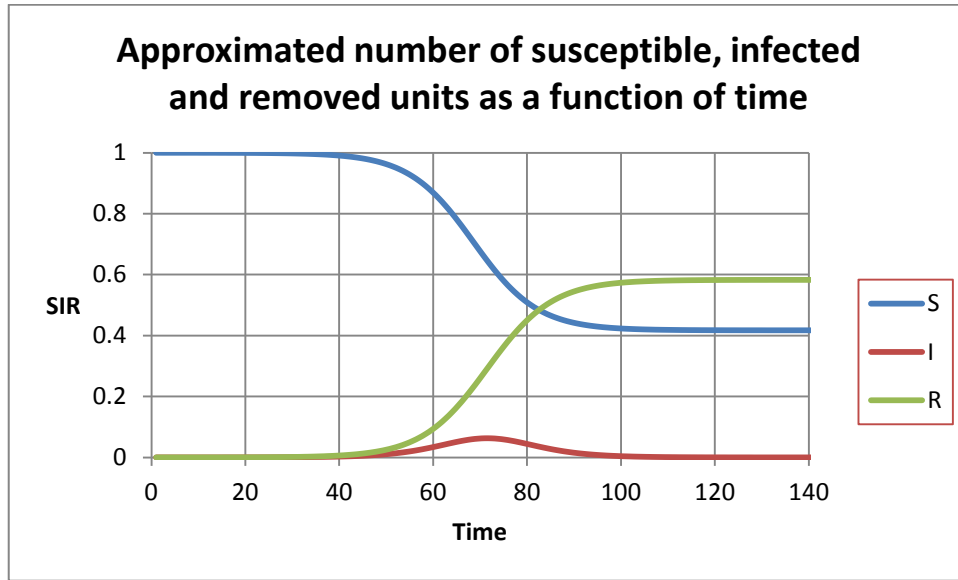


Figure 8: Number of susceptible, infected and removed units as a function of time.

One could argue that we can solve the original model numerically and store the results in look up tables instead of using an approximate & analytical model. There are at least four reasons not to use look up tables. First, the parameters  $a$  and  $b$  ( $O(N^2)$ ) need to be parametrized in order to obtain  $S$ ,  $I$  and  $R$  ( $O(N)$ ) as a function of time  $t$  ( $O(N)$ ) with specific boundary conditions ( $O(N)$ ). This necessitates a complexity of at least  $O(N^5)$  as opposed to  $O(N)$  for the time span of the analytical model. Second, the ranges of the parameters  $a$  and  $b$  are not always known ahead of time and hence it is not always



possible to have look up tables for unexpected values of  $a$  and  $b$ . This, however, is not a problem for the analytical model. Third, as shown in the next section, we can determine the properties of the infection analytically such as the maximal number of infections ( $I_{\max}$ ) or the time when the infection dies out ( $I \leq \varepsilon$ ). This gives insights into the process of infection and the remedy to such an infection. Fourth, as shown above, the approximate analytical solution is very accurate and reproduces all of the features of the original model.

Note that these results were also reported in Ref [17].

## 6 Properties of the Approximated Solution

---

### 6.1 Number of infected units

From basic calculus, the maximum of  $I(t)$  occurs at:

$$t = \frac{1}{\sqrt{\Delta}} \ln \left( -\frac{f_2}{f_1} \right) \quad (35)$$

where  $\frac{d}{dt}I = 0$ . Hence,

$$I_{\max} = -\frac{c}{4} \quad (36)$$

We can determine when  $I(t) = \varepsilon < I_{\max}$ , i.e. before the peak and after the peak:

$$\frac{cf_1f_2e^{\sqrt{\Delta}t}(f_1-f_2)^2}{(f_2-f_1e^{\sqrt{\Delta}t})^2} = \varepsilon < I_{\max} \quad (37)$$

Let  $\lambda = -f_1/f_2e^{\sqrt{\Delta}t}$ , where  $\lambda$  satisfies:

$$\lambda^2 + \lambda \left( 2 + c \frac{(f_1-f_2)^2}{\varepsilon} \right) + 1 = 0 \quad (38)$$

which generates:

$$\lambda_{\pm} = \frac{-\left( 2 + \frac{c}{\varepsilon}(f_1-f_2)^2 \right) \pm \sqrt{\left( 2 + \frac{c}{\varepsilon}(f_1-f_2)^2 \right)^2 - 4}}{2} \quad (39)$$

This corresponds to:

$$t_{\pm} = \ln \left( -\frac{f_2}{f_1} \lambda_{\pm} \right) \quad (40)$$

## 6.2 Limits as $t \rightarrow \infty$

To investigate the long term effects of the system, we evaluate the SIR as time tends to infinity.

$$\lim_{t \rightarrow \infty} I(t) = \lim_{t \rightarrow \infty} \frac{cf_1 f_2 e^{\sqrt{\Delta t}} (f_1 - f_2)^2}{(f_2 - f_1 e^{\sqrt{\Delta t}})^2} = 0 \quad (41)$$

$$\lim_{t \rightarrow \infty} S(t) = \lim_{t \rightarrow \infty} S_0 e^{-a \frac{f_2(-1+e^{\sqrt{\Delta t}})}{-f_2/f_1 + e^{\sqrt{\Delta t}}}} = S_0 e^{-af_2} \quad (42)$$

$$\lim_{t \rightarrow \infty} R(t) = \lim_{t \rightarrow \infty} b \frac{f_2(-1+e^{\sqrt{\Delta t}})}{-f_2/f_1 + e^{\sqrt{\Delta t}}} = bf_2 \quad (43)$$

Note that the long term effects were also reported in Ref [17].

## 6.3 Further corrections

We note the quadratic approximation is symmetrical with respect to the vertex of the corresponding parabola. We could add another modelling parameter  $\delta$  to mimic the asymmetry of Equation (9). For example, we could modify Equation (26) to:

$$\frac{df}{dt} = \frac{c(f-f_1)(f-f_2)}{1+\delta f} \quad (44)$$

The expression  $1+\delta f$  induces the asymmetry. The parameters  $c$  and  $\delta$  can be derived by minimizing the  $\chi^2$ .

$$\begin{aligned} \frac{d}{dc} \int_0^{f_2} df \left\{ \frac{c(f-f_1)(f-f_2)}{1+\delta f} - (-bf - S_o e^{-af} + 1) \right\}^2 &= 0 \\ \frac{d}{d\delta} \int_0^{f_2} df \left\{ \frac{c(f-f_1)(f-f_2)}{1+\delta f} - (-bf - S_o e^{-af} + 1) \right\}^2 &= 0 \end{aligned} \quad (45)$$

This modifies Equation (27):

$$\frac{(1+\delta f)df}{c(f-f_1)(f-f_2)} = dt \quad (46)$$

Integrating both sides of Equation (46), we get:

$$\frac{1}{\sqrt{\Delta}} \ln \left( \frac{f-f_1}{f_2-f} \right) + \frac{\delta \cdot [f_1 \cdot \ln(f-f_1) - f_2 \cdot \ln(f_2-f)]}{\sqrt{\Delta}} = t + C \quad (47)$$

where  $C$  is a constant of integration. We can raise both sides of Equation (47) as powers of  $e$ . That is,

$$\frac{f-f_1}{f_2-f} e^{\delta [f_1 \cdot \ln(f-f_1) - f_2 \cdot \ln(f_2-f)]} = A e^{\sqrt{\Delta} t} \quad (48)$$

where  $A$  is a constant of integration. The correction for asymmetry emerges as:

$$e^{\delta [f_1 \cdot \ln(f-f_1) - f_2 \cdot \ln(f_2-f)]} \quad (49)$$

We expect  $\delta$  to be small since the quadratic function is very similar to Equation (26) as shown in Figure 3. Expanding Equation (49) as a Taylor series in  $f$ , we get:

$$e^{\delta [f_1 \cdot \ln(f-f_1) - f_2 \cdot \ln(f_2-f)]} = \frac{(-f_1)^{\delta f_1}}{(f_2)^{\delta f_2}} \left[ 1 + \frac{\delta f^2 (f_1 - f_2)}{2 f_1 f_2} \right] \quad (50)$$

Substituting the above into Equation (48), we get:

$$\left\{ \frac{(-f_1)^{\delta_{f_1}}}{(f_2)^{\delta_{f_2}}} \left[ 1 + \frac{\delta f^2 (f_1 - f_2)}{2 f_1 f_2} \right] \right\} \frac{f - f_1}{f_2 - f} = A e^{\sqrt{\Delta} t} \quad (51)$$

We observe that the zeroth order correction,  $\frac{(-f_1)^{\delta_{f_1}}}{(f_2)^{\delta_{f_2}}}$ , can be absorbed into the parameter  $A$ . That is,

$A = \frac{(-f_1)^{\delta_{f_1}+1}}{(f_2)^{\delta_{f_2}+1}}$  instead of  $A = \left( \frac{-f_1}{f_2} \right)$ . The first order (linear) correction, i.e.  $O(f)$ , is zero because there is no  $f$  term. The first nontrivial correction is the second order term, i.e.  $O(f^2)$ . Therefore, by scaling  $A$  we get a correction to the first order. The correction  $O(f^2)$  will be presented in the future.

Another approach to induce asymmetry that we have examined is to consider:

$$\frac{df}{dt} = c (f - f_1)^{1-\delta_1} (f_2 - f)^{1+\delta_2} \quad (52)$$

We will report this in a future report.

## 7 Conclusion

---

In this SR, we have derived an approximated SIR model and found the corresponding analytical solution. We could consider the approximated SIR model itself a SIR model. After all, the exact SIR model is a man-made model where the couplings among the susceptible units, the infected units and the removed units are parts of the modelling.

Unlike the exact SIR model and in spite of its simplicity, the analytical nature of the approximate solution allows one to determine the long term characteristics of the SIR units, the maximum number of infected units and the time when this occurs with only three parameters  $c, f_1, f_2$  (the three parameters of a quadratic function) and the boundary conditions.  $c, f_1, f_2$  are obtained from the couplings  $a, b$  of the exact SIR model and the boundary conditions.

We draw a parallelism to Little's law (Ref [29]) in queuing theory which is very simple but also very useful because of its simplicity and applicability to queuing analyses. For this reason, we purposely minimize the level of details and do not model the specifics of a virus propagation.

This allows us to plan for cyber-attacks. Knowing  $c, f_1, f_2$ , we can determine the extent of the damage, i.e. the number of infected units, the number of susceptible units and the number of removed units as functions of time. These numbers are illustrated in Figure 4, Figure 5 and Figure 6, respectively. They show how long the system takes to recover, e.g. when the number of infected units reaches a minimum acceptable value after attaining a maximum value.

A capable enemy would integrate a cyber-attack with a missile attack for example. To counter such a combined attack, the defence needs to know the extent of the damage due to the cyber-attack. The defence could lose its net centric capabilities and hence may engage the incoming missiles in an uncoordinated way or even simply launch its interceptors in the wrong direction. As a result, the defence will suffer degradations in its effectiveness, Ref [30]. In real terms, this can be translated into the difference between success or failure, life or death.

In the future, we will examine the impact of such a combined attack where the parameters  $a$  and  $b$  assume realistic values. We will determine the timeline, the damage to the defence and the change in measures of effectiveness such as the probability of raid annihilation due to the integration of a cyber-attack and a missile attack.

## References

---

- [1] Symantec. Viruses that can cost you? (online), [http://www.symantec.com/region/reg\\_eu/resources/virus\\_cost.html](http://www.symantec.com/region/reg_eu/resources/virus_cost.html) (Access date: 26 Oct 2016).
- [2] Smith?, R. Modelling disease ecology with mathematics, American Institute of Mathematical Sciences, 2008.
- [3] Greenberg, A. Hackers remotely kill a Jeep on the highway—with me in it, 21 Jul 2015 (online), <https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/> (Access date: 26 Oct 2016).
- [4] Greenberg, A. The Jeep hackers are back to prove car hacking can get much worse, 01 Aug 2016 (online), <https://www.wired.com/2016/08/jeep-hackers-return-high-speed-steering-acceleration-hacks/> (Access date: 26 Oct 2016).
- [5] Greenberg, A. Hackers can disable a sniper rifle—or change its target, 29 Jul 2015 (online), <https://www.wired.com/2015/07/hackers-can-disable-sniper-riflor-change-target/> (Access date: 26 Oct 2016).
- [6] Sanger, D. A eureka moment for two Times reporters: North Korea’s missile launches were failing too often, *The New York Times*, 06 Mar 2017.
- [7] Blake, A. The first Trump-Clinton presidential debate transcript, annotated, *The Washington Post*, 26 Sep 2016 (online), <https://www.washingtonpost.com/news/the-fix/wp/2016/09/26/the-first-trump-clinton-presidential-debate-transcript-annotated/> (Access date: 27 Oct 2016).
- [8] The global risks report 2016, 11th ed., World Economic Forum (online), <http://reports.weforum.org/global-risks-2016/executive-summary/> (Access date: 26 Oct 2016).
- [9] McAfee. Net losses: estimating the global cost of cybercrime, Centre for strategic and international studies, Jun 2014 (online), <http://www.mcafee.com/ca/resources/reports/rp-economic-impact-cybercrime2.pdf> (Access date: 27 Oct 2016).
- [10] Kesan, J. and Hayes, C. Mitigative counterstriking: self-defense and deterrence in cyberspace, *Harvard Journal of Law and Technology*, Vol. 25, No. 2 (Spring 2012), pp. 429–543 (Available at SSRN: <http://ssrn.com/abstract=1805163>).
- [11] NATO. NATO fact sheet (online). [http://www.nato.int/nato\\_static\\_fl2014/assets/pdf/pdf\\_2016\\_07/20160627\\_1607-factsheet-cyber-defence-eng.pdf](http://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_07/20160627_1607-factsheet-cyber-defence-eng.pdf) (Access date: 26 Oct 2016).
- [12] Krishnan, G. S. S., et al. Computational intelligence, cybersecurity and computational models: proceedings of ICC3, Springer, 2013.
- [13] Xu, S., Lu, W., and Li, H. A stochastic model of active cyber defense dynamics, *Internet Mathematics*, Vol. 11 (Jan 2015), pp. 28–75.

- [14] Keeling, M.J. and Rohani, P. Modeling Infectious Diseases in Humans and Animals, Princeton University Press, 2007.
- [15] Wikipedia. Compartmental models in epidemiology (online), [https://en.wikipedia.org/wiki/Epidemic\\_model](https://en.wikipedia.org/wiki/Epidemic_model), (Access date: 20 Aug 2016).
- [16] Hethcote, H. The mathematics of infectious diseases, *SIAM Review*, Vol. 42, No. 4 (2000), pp. 599–653.
- [17] Nguyen, B. Modelling cyber vulnerability using epidemic models, *7th International Conference on Simulation and Modeling Methodologies, Technologies and Applications Proceedings*, Madrid (Spain), 26–28 Jul 2017.
- [18] Morris-King, J. and Cam, H. Ecology-inspired cyber risk model for propagation of vulnerability exploitation in tactical edge, *Proceedings of the IEEE 2015 Military Communications Conference MILCOM'2015*, 2015, pp. 336–341.
- [19] Zou, C. C., Gong, W., and Towsley, D. Code red worm propagation modeling and analysis, *Proceedings of the 9th ACM conference on Computer and communications security*, 2002, pp. 138–147.
- [20] Bailey, N. T. J. The mathematical theory of infectious diseases and its applications, Charles Griffin & Company LTD, 2nd ed.
- [21] Horton J. and Seberry, J. Computer Viruses: an Introduction, *Proceedings of the Twentieth Australasian Computer Science Conference (ACSC'97)*, Aust. Computer Science Communications, Vol. 19, No. 1 (Feb 1997), pp. 122–131.
- [22] Chen, Z., Gao, L., and Kwiat, K. Modeling the spread of active worms, *IEEE INFOCOM 2003. Twenty-second Annual Joint Conference of the IEEE Computer and Communications Societies*, (IEEE Cat. No.03CH37428), Vol.3 (2003), pp. 1890–1900.
- [23] Khan, M. S. S. A computer virus propagation model using delay differential equations with probabilistic contagion and immunity, *International Journal of Computer Networks & Communications*, Vol.6, No.5 (Sep 2014), pp. 111–128.
- [24] Bondy, J. A. and Marty, U. S. R. Graph theory. Springer, 2008.
- [25] Ganesh, A., Massoulie, L., and Towsley, D. The effect of network topology on the spread of epidemics, *Proceedings of IEEE Infocom*, 2005.
- [26] Chakrabarti, D., Wang, Y., Wang, C., Leskovec, J., and Faloutsos, C. Epidemic thresholds in real networks, *Association for Computing Machinery Transaction Information System Security*, Vol. 10, No. 4 (2008), pp. 1–26.
- [27] Higham, N. J., et al., eds. The Princeton companion to applied mathematics, Princeton University Press, 2015.



- [28] Gradshteyn, I. S., and Ryzhik, I. M. Tables of integrals, series, and products, 6th ed. Academic Press, San Diego, CA., 1979.
- [29] Little, J. D. C. A proof for the queuing formula  $L = \lambda \cdot W$ , *Operations Research*, Vol. 9, No. 3 (1961), pp. 383–387.
- [30] Nguyen, B. U. and Miah, S. Comparison of metrics for missile defence between perfect coordination and no coordination, Defence Research and Development Canada, Scientific Report, DRDC-RDDC-2015-R228, Oct 2015.

## List of symbols/abbreviations/acronyms/initialisms

---

$a$	Rate of infection
$A$	Constant of integration
$b$	Rate of recovery
$c$	The coefficient of degree two for a parabola equation
$C$	Constant of integration
$\delta$	A parameter that induces asymmetry in the approximate solution
$\Delta$	Discriminant of a quadratic equation
DRDC	Defence Research and Development Canada
$f$	Integral of the number of infected units
$f_1, f_2$	Roots to a differential equation
$I$	Number of infected units
$I_0$	Number of infected units at time zero
$I_{\max}$	Maximum number of infected units
$N$	Total number of units
$R$	Number of recovered units
$R_0$	Number of recovered units at time zero
$S$	Number of susceptible units
$S_0$	Number of susceptible units at time zero
SEIR	Susceptible-Exposed-Infected-Removed
SIR	Susceptible-Infected-Recovered model
SIS	Susceptible-Infectious-Susceptible
SR	Scientific Report
$t$	Time
$W$	Lambert function
$z$	A parameter in the expansion of Lambert function

DOCUMENT CONTROL DATA		
(Security markings for the title, abstract and indexing annotation must be entered when the document is Classified or Designated)		
1. ORIGINATOR (The name and address of the organization preparing the document. Organizations for whom the document was prepared, e.g., Centre sponsoring a contractor's report, or tasking agency, are entered in Section 8.)  <b>DRDC – Centre for Operational Research and Analysis            Defence Research and Development Canada            101 Colonel By Drive            Ottawa, Ontario K1A 0K2            Canada</b>		2a. SECURITY MARKING (Overall security marking of the document including special supplemental markings if applicable.)  <b>CAN UNCLASSIFIED</b>
		2b. CONTROLLED GOODS  <b>NON-CONTROLLED GOODS            DMC A</b>
3. TITLE (The complete document title as indicated on the title page. Its classification should be indicated by the appropriate abbreviation (S, C or U) in parentheses after the title.)  <b>Modelling cyber vulnerability using epidemic models</b>		
4. AUTHORS (last name, followed by initials – ranks, titles, etc., not to be used)  <b>Nguyen, B.</b>		
5. DATE OF PUBLICATION (Month and year of publication of document.)  <b>May 2018</b>	6a. NO. OF PAGES (Total containing information, including Annexes, Appendices, etc.)  <b>32</b>	6b. NO. OF REFS (Total cited in document.)  <b>30</b>
7. DESCRIPTIVE NOTES (The category of the document, e.g., technical report, technical note or memorandum. If appropriate, enter the type of report, e.g., interim, progress, summary, annual or final. Give the inclusive dates when a specific reporting period is covered.)  <b>Scientific Report</b>		
8. SPONSORING ACTIVITY (The name of the department project office or laboratory sponsoring the research and development – include address.)  <b>DRDC – Centre for Operational Research and Analysis            Defence Research and Development Canada            101 Colonel By Drive            Ottawa, Ontario K1A 0K2            Canada</b>		
9a. PROJECT OR GRANT NO. (If appropriate, the applicable research and development project or grant number under which the document was written. Please specify whether project or grant.)		9b. CONTRACT NO. (If appropriate, the applicable number under which the document was written.)
10a. ORIGINATOR'S DOCUMENT NUMBER (The official document number by which the document is identified by the originating activity. This number must be unique to this document.)  <b>DRDC-RDDC-2017-R213</b>		10b. OTHER DOCUMENT NO(s). (Any other numbers which may be assigned this document either by the originator or by the sponsor.)
11a. FUTURE DISTRIBUTION (Any limitations on further dissemination of the document, other than those imposed by security classification.)  <b>Public release</b>		
11b. FUTURE DISTRIBUTION OUTSIDE CANADA (Any limitations on further dissemination of the document, other than those imposed by security classification.)		

12. **ABSTRACT** (A brief and factual summary of the document. It may also appear elsewhere in the body of the document itself. It is highly desirable that the abstract of classified documents be unclassified. Each paragraph of the abstract shall begin with an indication of the security classification of the information in the paragraph (unless the document itself is unclassified) represented as (S), (C), (R), or (U). It is not necessary to include here abstracts in both official languages unless the text is bilingual.)

This Scientific Report (SR) documents an epidemic model known as SIR (Susceptible-Infected-Removed units). We derive an approximated solution to the differential equations that define the SIR model. Unlike the exact SIR solution, the approximate solution is analytical and has a close form expression. We use this approximate model as an inspiration to cyber defence. Such a model allows us to investigate the characteristics of the propagation of electronic viruses. That is, we can determine the number of susceptible units, the number of infected unit and the number of removed units as a function of time. This information will eventually permit the defence to find ways to eradicate a virus attack.

-----

Ce rapport scientifique fait état d'un modèle épidémique appelé SIR (Sensible-Infecté-Retiré). Nous obtenons une solution approximative aux équations différentielles qui définissent le modèle SIR. Contrairement à la solution SIR exacte, la solution approximative est analytique et elle a une expression en forme fermée. Nous utilisons ce modèle approximatif comme inspiration pour la cyberdéfense. Un tel modèle nous permet d'étudier les caractéristiques de la propagation de virus électroniques. C'est-à-dire que nous pouvons déterminer le nombre d'unités sensibles, le nombre d'unités infectées et le nombre d'unités retirées en fonction du temps. Cette information permettra ensuite à la défense de trouver des façons d'éradiquer une attaque virale.

13. **KEYWORDS, DESCRIPTORS or IDENTIFIERS** (Technically meaningful terms or short phrases that characterize a document and could be helpful in cataloguing the document. They should be selected so that no security classification is required. Identifiers, such as equipment model designation, trade name, military project code name, geographic location may also be included. If possible keywords should be selected from a published thesaurus, e.g., Thesaurus of Engineering and Scientific Terms (TEST) and that thesaurus identified. If it is not possible to select indexing terms which are Unclassified, the classification of each should be indicated as with the title.)

cyber defence; epidemic models; infectious diseases