Mathematical Models of Malware Propagation: A Critical Level of Protection (CLoP)

Asep K. Supriatna, Hennie Husniah, R.A.R. Harry Anwar, and Mokhamad Hendayun

***Abstract*— The use of the Internet to undertake violent acts that threaten loss of life or other forms of unwanted effects, such as data loss, potential economic loss, and insecure situations is alarming. This includes the attack to personal computers attached to the Internet by sending unwanted objects, such as computer viruses, computer worms, phishing, and other malicious software. This paper presents a mathematical model of the dynamics of the propagation of malwares or computer viruses on a computer network. The model is inspired by an *SIR* model in epidemiology, in which here the computer population in the network is divided into several subpopulations to include the susceptible (*S*), infected (*I*), and recovered (*R*) subpopulations. Mathematically, the SIR type model forms a system consisting of coupled differential equations to describe the infection process among subpopulations. Standard tools and analysis from dynamical system theory usually are utilized to find both the transient and equilibrium solutions of the models under investigation. We are especially interested in determining the long-term status of a computer network, whether the network will be free from the malware/virus or persists with the infection of the malware/virus, whenever anti-malware or anti-virus is given to some susceptible computers as an attempt to protect the computers from the malware or virus attack. Threshold parameters to determine the long-term status of the system will be investigated for *SIR* model and some of its generalization such as *SEIR*, *SEIQRS*, and *SEIIQR*.**

***Index Terms*— basic reproduction number, computer virus, critical level of protection (CloP), malware, mathematical model.**

I. INTRODUCTION

NOWADAYS terrorism appears in many different forms. One of them is the attack and threat to a network of computers by sending various unwanted malicious objects such as viruses, malwares, etc. The objects are sent to infect a computer and the infected computer propagates the object to other computers through a network. This propagation resembles the transmission of infectious disease in human and other living creatures. No wonder that the way on how to understand the transmission and to control the malicious object adopts some ideas from Mathematical Epidemiology, the more matured discipline compared to the one that studies the propagation of malicious objects in computer networks at the time.

In Mathematical Epidemiology, the first mathematical model to study the transmission of contagious disease back to 1926-1927, when Kermack and McKendrick proposed a model which in the modern days is called the SIR (Susceptible-Infected-Removed) model [1], [2]. A brief and good introductory to the theory is given in [3] which overviews the historical development of the theory. More advanced treatment can be read in [4], which also contains other biological problems, and more specific materials can be found in [5], [6], which present rich methods in mathematical epidemiology.

It is not clear when is the first use of the theory in Computer Science, but the references [7]-[10] are among the early works who used the theory for the transmission of computer viruses. Recently the references on the use of this mathematical method and its extension and refinement are very vast, among others are [11]-[18]. We give a brief review of the mathematical method of the SIR model in the following section.

II. METHOD

We use a mechanistic mathematical modeling in studying the propagation of a malware in a network of computers. We follow the method of [1] and [2] to construct the SIR mathematical model of the malware propagation by mimicking the malware propagation as if a disease transmission in human population.

In their model the authors in [1] and [2] assume that the population under investigation is divided into three subpopulations: subpopulation contains those healthy individuals yet susceptible to the disease (*S*), subpopulation contains those infected individuals (*I*), and subpopulation contains those individuals recovered from the disease (*R*). The model has the form in a system of three differential equations, $S'(t)$, $I'(t)$, and $R'(t)$, representing the rates of change for the respective subpopulations. Now let us see the transmission in a network perspective as follows. Let us assume a computer networks consists of *N* unit of computers. The number of

Manuscript received September 20, 2019.

This work was supported by Ministry of Research, Technology and Higher Education of the Republic of Indonesia who has funded the work through the scheme of PDUPT 2019 to AKS with contact number 2827/UN6.D/LT/2019.

A. K. Supriatna is with the Applied Mathematics, Padjadjaran University, Sumedang 45363, Indonesia (e-mail: a.k.supriatna@unpad.ac.id).

H. Husniah is with the Industrial Engineering Department, Langlangbuana University, Bandung 40261 Indonesia (corresponding author e-mail: hennie.husniah@gmail.com).

R.A.R. Harry Anwar, is with the Police Science Department, Langlangbuana University, Bandung 40261 Indonesia (e-mail: anggororahardjo@gmail.com).

M. Hendayun is with the Informatics Engineering Graduate Program, Langlangbuana University, Bandung 40261 Indonesia (email: hendayun@aol.de).

susceptible, infected, and recovered computers at time t is $S(t)$, $I(t)$, and $R(t)$, respectively (for the SIR model), with $S(t) + I(t) + R(t) = N$. Upon the completion of the model development and analyis, we proceed by modifying the model to more realistic cases, such as SEIR, SEIQRS, and SEIIQR. We look for the endemic equilibrium solution for each model and solve the critical protection level from the resulting endemic equilibrium by relating it to the basic reproduction number of each model. The following section present the results for the SIR model and it's modification in the forms of SEIR, SEIQRS, and SEIIQR models.

III. Results and Discussions

3.1 SIR Model of Virus/Malware Transmission

Let us assume a computer networks consists of N unit of computers. The number of susceptible, infected, and recovered computers at time t is $S(t)$, $I(t)$, and $R(t)$, respectively, with $S(t) + I(t) + R(t) = N$. The SIR model is governed by a system of differential equations :

$$S' = -\beta SI\,,\; I' = \beta SI - kI\,, \text{ and } R' = kI \tag{1}$$

with β represents the number of contacts per unit time that are sufficient to spread the virus/malware to other computers. If we assume a homogeneous mixing of the computers in the network, on average, each infected individual generates $\beta\, S$(t) new infected computers, so that the rate of conversion of susceptible computers to infected computers is $\beta\, S$(t) I(t). We then assume that a fixed fraction γ of the infected group will recover during any given unit time, so that the rate of conversion of infected computers recovered computers is γ I(t).

The equilibrium solution is found by solving the equations $S' = 0$, $I' = 0$, and $R' = 0$ to obtain (S^*, I^*, R^*) with $S^* = k/\beta$, $I^* = 0$, and $R^* = 0$. In fact for $I^* = 0$ and $R^* = 0$, any values of S^* is the equilibrium solution. This equlibrium indicates that eventually the system will end up either with all susceptible computers are infected or only some of them are infected. In both cases the infection dies out eventually. We give an illustration for both cases with parameters $\beta = 0.0025$ and $g = 0.045$ (Fig. 1) in which not all of the computers are infected and $\beta = 0.025$ and $g = 0.045$ (Fig. 2) in which all of the computers are infected.

A. Deriving a protection level p

Recall that the positive equilibrium point is given by $S^* = k/\beta$, which tells us that eventually the number of uninfected computers, if there is no action to protect the network from the malware/virus, will be this number. Suppose that now we give a protection to the network, then the system will ends up to a new equilibrium, called S^{*p} which expected should be bigger than $S^* = \dfrac{k}{\beta}$ (there are more uninfected computers in the network due to the effect of protection), hence $S^{*p} \geq S^* = \dfrac{k}{\beta}$. This condition can be achieved for example by lowering the value of β to a new level, say $(1-p)\beta$ with $0 < p < 1$ so that $S^{*p} = \dfrac{k}{(1-p)\beta} > S^*$. The last condition is always satisfied by any chosen protection level p with $0 < p < 1$.

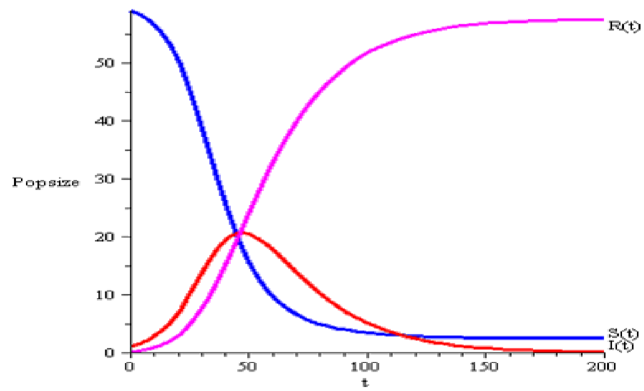

Fig. 1. Plots of S, I, and R for SIR-1 model with low β.

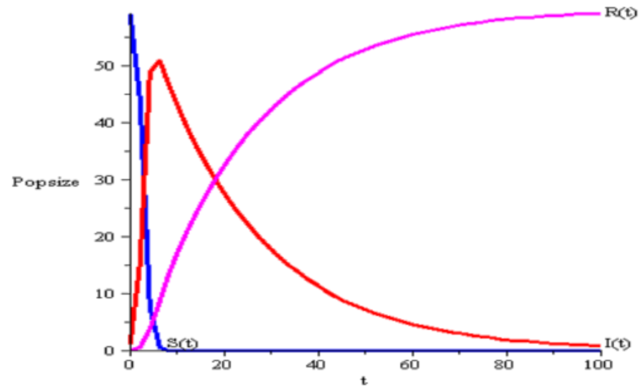

Fig. 2. Plots of S, I, and R for SIR-1 model with high β.

B. Another form of SIR model

The SIR model has been modified to many directions, for example by introducing procurement of new susceptible computers to the network (Π), while also considering some computers that are discarded from the network due to their obsolete or damage (δ), and a more realistic force of infection β that takes account the probability of succesful contact with susceptible computers (with other types of computers, infected or recovered). In a normalized form, the model now may looks like:

$$S' = \Pi - \beta SI - \delta S\,,\; I' = \beta SI - kI - \delta I\,, \text{ and } R' = kI - \delta R \tag{2}$$

with the malware/virus-free equilibrium solution is (S^*, I^*, R^*) with $S^* = \dfrac{\Pi}{\delta}$, $I^* = 0$, and $R^* = 0$ and the endemic equilibrium solution is (S^e, I^e, R^e) with $S^e = \dfrac{(k+\delta)}{\beta}$, $I^e = \dfrac{\delta}{\beta}\left(\dfrac{\Pi\beta}{\delta(k+\delta)} - 1\right)$, and $R^e = \dfrac{k}{\delta} I^e$. Note that the equilibrium solution of infected computers exists only if $R_o = \dfrac{\Pi\beta}{\delta(k+\delta)} > 1$. Unlike the first form of the SIR model, in which the equilibrium solution of the infected computers is zero, here there is a number R_o, which has a property as a threshold number with the threshold value 1. It is determining the existence and nonexistence of the endemic equilibrium I^e. Hence it is plausible to concept that any protection is directed to make the endemic equilibrium dissapear (equivalent by saying that the effective R_o - the new R_o in the present of protection level p - is less than one). There are many papers discussing the stability of this equilibrium with the relation to this threshold. Mathematical epidemiology literatures call this threshold as the basic reproduction number.

C. Deriving the critical protection level p of another form of SIR model

As mentioned above any action of protection is technically directed to lowering the basic reproduction number so that it is less than one. This can be done for example by lowering the attack rate/the force of infection from β to $(1\text{-}p)\beta$ with $0 < p < 1$. Subtituting this value into the model will give rise to the effective basic reproduction number $R_p = \dfrac{(1-p)\Pi\beta}{\delta(k+\delta)}$.

This number should be less than one, to guarantee that the endemic equilibrium will dissapear. Solving this for p will end up to $p > p^* = 1 - 1/R_o = \dfrac{\Pi\beta\delta(k+\delta)-1}{\Pi\beta\delta(k+\delta)}$. We will call this p as the critical level of protection (CloP). Any protection level greater than this CLoP will eliminate the spread of the malware/virus, while any protection level lower than this CLoP will not able to eliminate the spread of malware/virus.

As an illustration we give numerical examples. Fig. 3 shows the plots of S, I, and R subpopulations with low malware/virus infection rate ($\beta = 0.045$, $k = 0.045$, $\mu = 0.1$, $k = 0.045$, $\Pi = 0.25$, with the resulting basic reproduction number R_o is less than one) and Fig. 4 shows the plots of S, I, and R subpopulations with high malware/virus infection rate ($\beta = 0.25$, $k = 0.045$, $\mu = 0.1$, $k = 0.045$, $\Pi = 0.25$ with the resulting basic reproduction number R_o is more than one). In Fig. 3, since eventually the malware/virus infection dies out, we do not have to do anything. However in Fig. 4, since the malware/virus infection is persisting in the network (endemic), a protection intervention should be done.

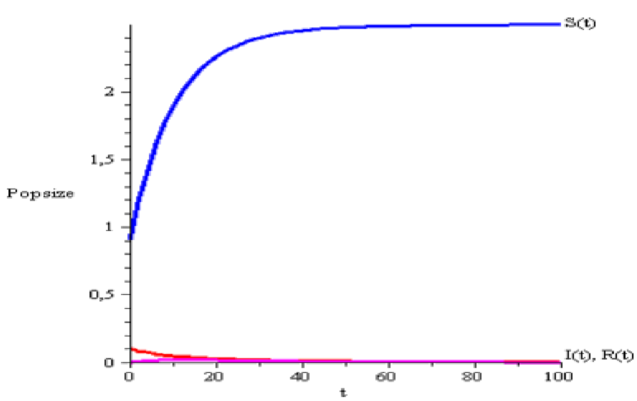

Fig. 3. Plots of S, I, and R for SIR-2 model with low β.

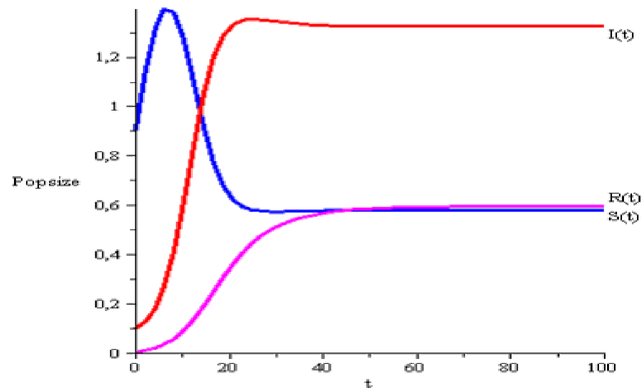

Fig. 4. Plots of S, I, and R for SIR-2 model with high β.

Fig. 5 shows the plots of S (susceptible computer subpopulation) with high malware/virus infection rate (as in Fig. 4) with various level of protections: no protection, low protection (lower than the sugested CLoP = p^*), and sufficient protection (higher than the suggested CLoP = p^*). Sufficient protection at a level higher than the CLoP give a significant result in protecting the computers in the network. Fig. 6 shows the plots of I (infected computer subpopulation) with various rate of protections as in Fig. 5. It reveals that deploying protection at a level lower than the suggested rate will not able to eliminate the malware/virus infection in the long run. It is worth to note that there is a close relationship between the natural basic reproduction number with the suggested or critical level of protection, given by $p^* = 1 - 1/R_0$.

We note that a deployment of protection at the level higher than p^* will eliminate the malware/virus infection, otherwise (i.e. a protection lower than this value) will make the infection remain persists in the network (endemic). This rules of thumb is true for all cases of p, and can be proved mathematically. This is among the important finding in the theory of computer epidemiology. The following section will investigate the rules of thumb for different models.

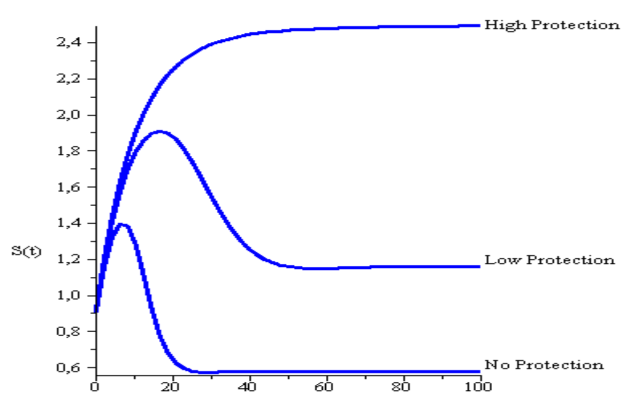

Fig. 5. Plots of S for SIR-2 model with high β.

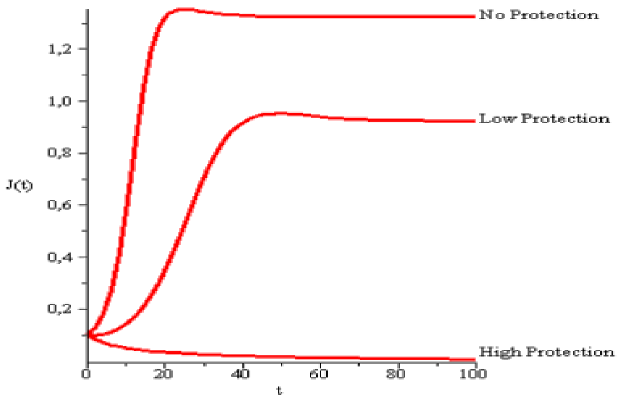

Fig. 6. Plots of I for SIR-2 model with high β.

3.2 Extensions of SIR Model

The SIR model is the simplest mathematical form of the malware/virus transmission equation in a network. There are many direction in extending the SIR model. Some examples are [15] introduced the protected class explicitly into the SIR model, [13] introduced several human interventions in the SIR model, some authors refined the model by introducing exposed class of computers to make the SIR model more realistic, such as [11], [18], some authors adding different route of infection, such as the vertical transmission [12], some authors considered reinfection due to the loss of immunity after longtime recovery [14], some works present the SIR model in the contex of fractional-order delayed malware propagation [16]. In this section we review some of the extended model by relating it to the concept of CLoP we introduced here.

The authors in [11] proposed a SEIQRS model for the transmission of malicious object in computer network. They assumed that the population of computer in the network is divided into susceptible (S), exposed (E), infected (I), quarantine (Q), and recovered/removal (R) classes. In this model, after the run of anti-malicious software, the computer network becomes temporary recovered but they will move to the susceptible class due to the loss of immunity after a certain period. The model is governed by the following system of differential equations

$$S' = A - \beta SI - \delta S + \eta R \qquad (3.a)$$

$$E' = \beta SI - (d+\mu)E \qquad (3.b)$$

$$I' = \mu E - (d+\alpha+\gamma+\delta)I \qquad (3.c)$$

$$Q' = \delta I - (d+\alpha+\varepsilon)Q \qquad (3.d)$$

$$R' = \gamma I + \varepsilon Q - (d+\eta)R \qquad (3.d)$$

with $X' = \dfrac{dX}{dt}, X \in \{S, E, I, Q, R\}$.

They found the basic reproduction number, given by $R_{OQ} = \dfrac{\beta(A/d)}{\mu+\alpha+\delta+\gamma+d}$, and the malware-endemic equlibrium in the form of R_{OQ} (S^*, E^*, I^*, Q^*, R^*), with $S^* = \dfrac{A/d}{R_{OQ}}$, $E^* = \dfrac{d(R_{OQ}-1)}{\beta}$, $I^* = \dfrac{d(R_{OQ}-1)}{\beta}\dfrac{\mu}{d+\alpha}$, $Q^* = \dfrac{\delta(R_{OQ}-1)}{\beta}\left(\dfrac{\mu}{\varepsilon+d+\alpha}\right)$, and $R^* = \dfrac{(R_{OQ}-1)}{\beta}\left(\gamma + \dfrac{\varepsilon\delta\eta}{\eta+\varepsilon+d+\alpha}\right)$. By following the same procedure as before, the critical level of malware treatment is $p^* = \dfrac{\beta A - d(\mu+\alpha+\delta+\gamma+d)}{\beta A}$. We found the following theorem on deploying the malware/virus protection. We omit the proof since it is a direct consequence of the stability properties of the endemic state described in the original paper of [11].

Theorem 1: *Suppose that p is the level of malware/virus protection in a network with SEIQR malware/virus transmission model such that the effect of the protection is to reduce the basic reproduction number R_{OQ} to the effective reproduction number $R_{effQ} = \dfrac{\beta^p(A/d)}{\mu+\alpha+\delta+\gamma+d}$ with $\beta^p = (1-p)\beta$ for $0 < p < 1$ the following is true:*

a) If p is less than the critical level of protection $p^* = \dfrac{\beta A - d(\mu+\alpha+\delta+\gamma+d)}{\beta A}$ then the malware/virus will endemic in the network.

b) If p is more than the critical level of protection $p^* = \dfrac{\beta A - d(\mu+\alpha+\delta+\gamma+d)}{\beta A}$ then the malware/virus will dissapear from the network.

The following numerical examples are presented to give visual illustration of the results above and Theorem 1. We use two different data sets: Data Set 1 represents a low attack rate of malware/virus taken from [11] and Data Set 2 represents a high attack rate of malware/virus by modifying the Data Set 1 to obtain the basic reproduction number that greater than one as follows:

Data set 1:
{A = 0.3; d = 0.1; μ = 0.3; β = 0.3, ε = 0.3, γ = 1.8; η = 0.2; α = 0.2; δ = 3.8}
with S(0) = 200; E (0) = 0; I(0) = 1; Q(0) = 0; R(0) = 0.
Data set 2:
{A = 1.2; d = 0.05; μ = 0.15; β = 0.15, ε = 0.3, γ = 0.09; η = 0.2; α = 0.02; δ = 0.38}
With S(0) = 200; E (0) = 0; I(0) = 1; Q(0) = 0; R(0) = 0.

The solution for data sets 1 and 2 is shown in Fig. 7 and 8, respectively. Fig. 7 shows that the infected subpopulation will die out eventually. The basic reproduction number for this data set is R_{OQ} = 0.15. This means that there is nothing to do because the infected computer populations eventually goes to zero.

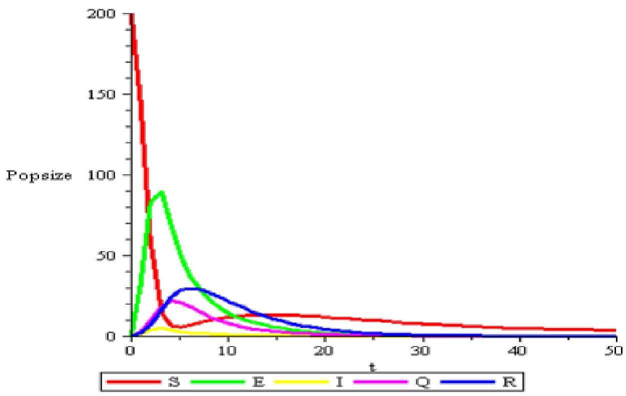

Fig. 7. Plots of all subpopulations for SEIQR model with low β (Data-Set 1). Reproduced from [11] with the same parameters, but probably different initial values.

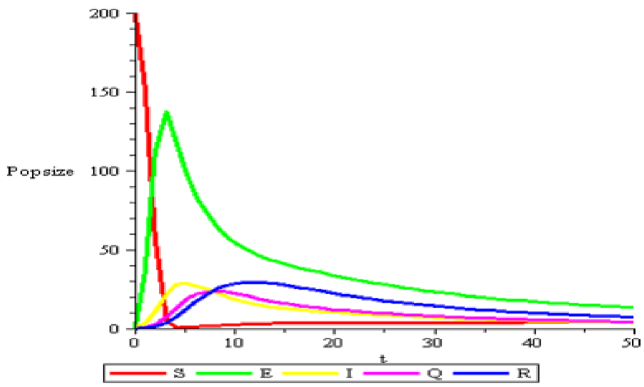

Fig. 8. Plots of all subpopulations for SEIQR model with high β (Data-Set 2).

Fig. 8 shows that the infected subpopulation (yellow) will be stable at a certain positive level eventually (in fact, it can be proved mathematically), besides there is an outbreak at t = 5. The basic reproduction number for this data set is $R_{OQ} = 5.22$. This means that there has something to do to drive the infected computer populations to go to zero, e.g. by giving anti malware/virus to some portion of susceptible computers subpopulation, say at the level of p. The theorem says that p should be bigger than $p^* = \dfrac{\beta A - d(\mu+\alpha+\delta+\gamma+d)}{\beta A} \approx 0.81$ (more than 81% of the susceptible computers must be "vaccinated").

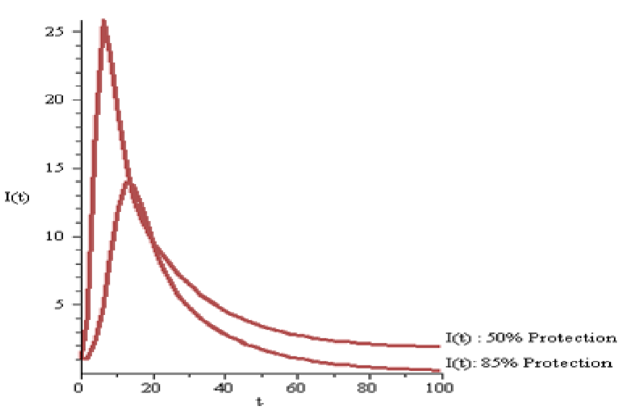

Fig. 9. Plots of all subpopulations for SEIQR model with high β (Data-Set 2).

Fig. 9 shows the solution when we set p below the threshold value (only 50% of the susceptible computers subpopulation is vaccinated) and above the threshold value (85% of the susceptible computers subpopulation is vaccinated). For 50% protection, there is still a high peak of outbreak (approximately 25 infected computers at time t=10 with a positive equilibrium in the long-term (2 infected computers). Meanwhile, for 85% protection although there is still an outbreak but the peak is lower (approximately 14 infected computers at time t = 17 and the long-term infection almost gone. If you do not happy with the result (because of the outbreak, then increase the protection level. The theory of the CLoP (critical level of protection) is directed only to control the long-term solution for the infected computers, not to the size of infection at certain time. This may be a subject for future investigation.

TABLE I
NETWORK EPIDEMIC MEASURES

Transmission Model	R_0	NESI as a function of R_0
SIR-1	$R_0 = \dfrac{\beta}{k}$	$I^e = 0$
SIR-2	$R_0 = \dfrac{\Pi\beta}{\delta(k+\delta)}$	$I^e = \dfrac{\delta}{\beta}\left(\dfrac{\Pi\beta}{\delta(k+\delta)} - 1\right)$
SEIR* [19]	$R_0 = \dfrac{A(\beta_1\alpha + \beta_1 c)}{abc}$	$I^* = \dfrac{A\alpha(R_O - 1)}{bcR_O}$
SEIQR [11]	$R_{OQ} = \dfrac{\beta(A/d)}{\mu+\alpha+\delta+\gamma+d}$	$I^* = \dfrac{d(R_{OQ}-1)}{\beta}\dfrac{\mu}{d+\alpha}$
SEIIQR [18]	$R_M = \beta\xi\dfrac{\sigma}{X_1}\dfrac{1}{X_2} + \beta\dfrac{\gamma}{X_1}\dfrac{X_4}{X_3X_4 - \eta\nu}$	$I_2^* = \dfrac{\gamma X_2 X_4}{\sigma(X_3X_4 - \eta\nu)} I_1^*$

Ro: Basic Reproduction Number
NESI: Natural Equilibrium State of Infection

We also compute the CLoP for other transmission models, such as SEIR, and SEIIQRS which are presented in Table I and Table II, but we do not go into the details since the derivation is analogous to previous models in the paper. Readers who would like to implement the theory are advised to read the original paper of the model as indicated in the references.

TABLE II
CRITICAL PROTECTION LEVELS

Transmission Model	Network Epidemic Measures CLoP
SIR-1	*none*
SIR-2	$p^* = \dfrac{\Pi\beta\delta(k+\delta) - 1}{\Pi\beta\delta(k+\delta)}$
SEIR* [19]	$p^* = \dfrac{A\beta(\alpha+c) - abc}{A\beta(\alpha+c)}$
SEIQR [11]	$p^* = \dfrac{\beta A - d(\mu+\alpha+\delta+\gamma+d)}{\beta A}$
SEIIQR [18]	$p^* = 1 - \dfrac{1}{R_M}$

CLoP: Critical Level of Protection
* The model assumes at any time, a computer is classified as internal and external depending on weather it is connected to internet or not.

IV. Conclusion

In this paper we have developed some mathematical models of malware/virus transmission in a network of computers. Several models, such as the SIR (type 1 and 2), SEIR, SEIQRS, and SEIIQRS are investigated. We did a standard procedure to obtain the basic reproduction number for each model and found the critical level of protection for each model that able to eliminate the malware/virus in the long run. The work ignore the cost of intervention. The inclusion of the cost of intervention is predicted could alter the critical level of protection. This is among the future research direction that worth to explore. The method can also be applied to other similar system such as those in [20].

Acknowledgment

We are grateful to the Ministry of Research, Technology, and Higher Education of the Republic of Indonesia who has funded the work through the scheme of PDUPT 2019 to AKS with contract number 2827/UN6.D/LT/2019.

References

[1] A.G. McKendrick, "Application of Mathematics to Medical Problems," *Proc. Ed. Math. Soc.*, vol. 44, pp. 98-130, 1926.

[2] W.O. Kermack and A.G. McKendrick, "Contributions to the Mathematical Theory of Epidemics," *Proc. Royal Soc. London,* vol. A115, pp. 700-721, 1927.

[3] N. Bacaër, "McKendrick and Kermack on epidemic modelling (1926–1927)," in *A Short History of Mathematical Population Dynamics,* Springer, London.

[4] J.D. Murray, "*Mathematical Biology,*" NewYork: Springer-Verlag, 3rd Edn., 2002.

[5] R.M. Anderson, R,M. May, and B. Anderson, "*Infectious Diseases of Humans: Dynamics and Control (Revised ed.)*," Oxford University Press, Oxford, UK, 1992.

[6] O. Diekmann, J.A.P. Heesterbeek, and T. Britton, "*Mathematical Tools for Understanding Infectious Disease Dynamics*," Princeton Series in Theoretical and Computational Biology, 2012.

[7] P. Pastor-Satorras and A. Vespignani, "Epidemic spreading in scale-free networks," *Phys. Rev. Lett.*, vol. 86, pp. 3200, 2001.

[8] A.L. Lloyd and R.M. May, "Epidemiology. How viruses spread among computers and people," *Science* vol. 18 292, pp. 1316-1317, 2001.

[9] J.L. Gondar and R. Cipolatti, "A mathematical model for virus infection in a system of interacting computers," *Comput. Appl. Math.*, vol. 22, no. 2, 2003.

[10] J.R.C. Piqueira, B.F. Navarro, and L.H.A. Monteiro, "Epidemiological models applied to virus in computer networks," *J. Comput. Sci.,* vol. 1, no. 1, pp. 31–34, 2005.

[11] B.K. Mishra and N. Jha, "SEIQRS model for the transmission of malicious objects in computer network," *Applied Mathematical Modelling*, vol. 34, pp. 710–715, 2010.

[12] B.K. Mishra and S.K. Pandey, "Effect of anti-virus software on infectious nodes in computer network: a mathematical model," *Physics Letters*, vol. A376, pp. 2389–2393, 2012.

[13] C. Gan, X. Yang, W. Liu, Q. Zhu, and X. Zhang, "Propagation of computer virus under human intervention: a dynamical model," *Discrete Dynamics in Nature and Society,* vol. 2012 Article ID 106950, 8 pages, 2012. doi:10.1155/2012/106950.

[14] B.K. Mishra and G.M. Ansari, "Differential epidemic model of virus and worms in computer network. *International Journal of Network Security*, vol. 14, no. 3, pp. 149-155, 2012.

[15] F. Abazari, M. Analoui, and H. Takabi, "Effect of anti-malware software on infectious nodes in cloud environment," *Computers and Security*, vol. 58, pp. 139-148, 2016.

[16] C. Xu, M. Liao, and P. Li, "Bifurcation of a fractional-order delayed malware propagation model in social networks. *Discrete Dynamics in Nature and Society*, vol. 2019, Article ID 7057052, 10 pages, 2019. doi: 10.1155/2019/7057052.

[17] M.Z. Ndii, B.S. Djahi, N.D. Rumlaklak, and A.K. Supriatna, "Determining the important parameters of mathematical models of the propagation of malware" *in Lecture Notes in Electrical Engineering Book Series*, vol. 565, pp. 1-9, 2019.

[18] A. Lanz, D. Rogers and T.L. Alford, "An epidemic model of malware virus with quarantine," *Journal of Advances in Mathematics and Computer Science*, vol. 33, no. 4, pp. 1-10, 2019.

[19] M. Peng, X. He, J. Huang, and T. Dong, "Modeling computer virus and its dynamics," Mathematical Problems in Engineering, vol. 2013, Article ID 842614, 5 pages, 2013, doi: 10.1155/2013/842614.

[20] A.K. Supriatna and H. Husniah, The critical level of intervention in controlling militant group related to terrorism, Proceedings of the 2nd International Conference on Education and Social Science Research (ICESRE 2019) in *Series:Advances in Social Science, Education and Humanities Research,* Atlantis Press, Available Online 24 March 2020, https://doi.org/10.2991/assehr.k.200318.028.