ISSN: 978-602-71169-7-9

Proceeding of 5th International Seminar on
New Paradigm and Innovation on Natural Science
and Its Application (5th ISNPINSA)

Mathematical Modeling of worm infection on computer in a Network: Case study in the Computer Laboratory, Mathematics Department, Diponegoro University, Indonesia

Nurfitriani S.[1,a], Widowati[1,b] , Robertus H.[1]

[1] Department of Mathematics, Faculty of Sciences and Mathematics, Diponegoro University,Semarang, Indonesia

[1,a] fitri.shin1@gmail.com, [1,b] wiwied_mathundip@yahoo.com

Abstract. Worm infection were an infection that attack a computer, it work by multiplied itself after got into a computer and made it over work and caused a computer to slowing down. Worm spreading infection describe by nonlinear mathematic model form with VEISV (Vulnerable, Exposed, Infected, Secured) as the model. Worm free equilibrium and endemic equilibrium were calculated to obtain the stability analysis, and numeric solution were performed using data from Computer Laboratory, Mathematics Department of Faculty of Sciences and Mathematics, Diponegoro University using Runge-Kutta fourth-order method. From the result of stability analysis we obtained that worm free equilibrium were not stable and endemic equilibrium were locally asymptotically stable, and from the result of numeric solution every class proportion from model were obtained.

Keywords: worm infection, VEISV model, stability analysis.

Introduction

According to Jose Nazario (2004), worms is an autonomous and independent infectious agent in replicate, it have the ability to infect a new computer system through a network facilities and the worm can propagate with or without the intervention of the user [1]. The concept work of the worm, first it had to find a gap to get into a new computer that has not been infected by the worm. After the worm gets in it will replicate itself in any folder or directory on hard drive, so the hard drive capacity becomes full. When the hard drive is full, it can lead to slower performance [2].

Worm on computer are built to propagate without warning or user interaction and cause Distributed denial of service (DDoS), leaking of information, financial loss and threatened the security of the information [3]. On November 2, 1988, the first worm named Morris was launched by Robert Tappan Morris and the Morris Worm was capable of infecting an estimated 60.000 computer, costing approximately $100 million damages [4]. Morris became the first person tried and convicted under the 1986 Computer Fraud and Abuse Act [5]. In 2001, the Code Red and Nimda worms quickly infected hundreds of thousands of computers, causing millions of dollars loss to our society [6]. On January 25, 2003 the slammer worm began to propagate and infected approximately 75.000 computer and achieved a full scanning rate of 55 million scan per second which caused network outages [7].

So far there is no way to prevent the worm propagation in a short period immediately after detecting the worm, thus current research focuses more on reducing the rate of propagation. The mathematical model can be used for security countermeasures [8]. The model of worm propagation have been modeled previously by researchers. One of them by Bimal Kumar Mishra and Samir Kumar Pandey, they investigated the fuzzy SIRS epidemic models for the worm propagation in computer networks [9].

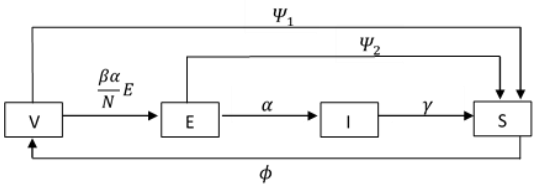
The Similarity between the spread of a biological virus and malicious worm propagation encourages the researcher to adopt an epidemic model to the network environment [10]. Mathematic model in the worm propagation, the number of computers are divided into four state, vulnerable (V), include all computer which are vulnerable to worm attack, exposed (E) include all computer which are exposed to worm attack, infectious (I) include all computer which are infected to worm attack and secured (S) include all computer which gained one or more security countermeasure.

ISSN: 978-602-71169-7-9

Mathematical model in this worm propagation are assumed there is no replacement occur and there is no dysfunction occur. The equilibrium were evaluated and analyzed the behavior of the system that can be determined by analyzing the stability of equilibrium solutions, then interpreting the results of the analysis into the real situation.

Mathematic Model

Worm is an infectious independent agent in replicate itself, worm has the ability to infect a computer without the knowledge of the user. Therefor, will be discussed the mathematical model that describes the worm propagation so the propagation rate can be reduced for the future. Below is the following diagram of the worm propagtion.



The parameters used in this model are, β is the contact rate, α is the state transition rate from E to I, Ψ_1 is the state transition rate from V to S, Ψ_2 is the state transition rate from E to S, γ is the state transition rate from I to S and ϕ is the state transition rate from S to V.

Transition process at vulnerable state

Suppose that at time t the number of vulnerable computers is $V(t)$ and at the time $(t+\Delta t)$ the number of vulnerable computers is $V(t+\Delta t)$. so the incidence of infection at the time Δt is $\frac{\beta\alpha}{N}EV$, State transition rate from vulnerable state to secured state at the time Δt is $\Psi_1 V\Delta t$ and the state transition rate from secured state to vulnerable state at the time Δt is $\phi S\Delta t$. The process of number of change in vulnerable state per unit time is as follows,

$$V(t+\Delta t) = V(t) - \frac{\beta\alpha}{N}EV\Delta t - \Psi_1 V\Delta t + \phi S\Delta t$$

$$V(t+\Delta t) - V(t) = -\frac{\beta\alpha}{N}EV\Delta t - \Psi_1 V\Delta t + \phi S\Delta t$$

$$V(t+\Delta t) - V(t) = (-\frac{\beta\alpha}{N}EV - \Psi_1 V + \phi S)\Delta t$$

$$\frac{V(t+\Delta t) - V(t)}{\Delta t} = -\frac{\beta\alpha}{N}EV - \Psi_1 V + \phi S$$

$$\frac{\Delta V}{\Delta t} = -\frac{\beta\alpha}{N}EV - \Psi_1 V + \phi S$$

$$\lim_{\Delta t\to 0}\frac{\Delta V}{\Delta t} = \lim_{\Delta t\to 0} -\frac{\beta\alpha}{N}EV - \Psi_1 V + \phi S$$

$$\frac{dV}{dt} = -\frac{\beta\alpha}{N}EV - \Psi_1 V + \phi S$$

So the state transition rate at vulnerable state is

$$\frac{dV}{dt} = -\frac{\beta\alpha}{N}EV - \Psi_1 V + \phi S \qquad (1)$$

Transition process at exposed state

Suppose that at time t the number of exposed computers is $E(t)$ and at the time $(t+\Delta t)$ the number of vulnerable computers is $E(t+\Delta t)$. so the incidence of infection at the time Δt is $\frac{\beta\alpha}{N}EV$, state transition rate from exposed state to infected state at the time Δt is $\alpha E\Delta t$, transition rate from exposed state to secured state at the time Δt is $\Psi_2 E\Delta t$. The process of number of change in exposed state per unit time is as follows,

$$E(t+\Delta t) = E(t) + \frac{\beta\alpha}{N}EV\Delta t - \alpha E\Delta t - \Psi_2 E\Delta t$$

$$E(t+\Delta t) - E(t) = \frac{\beta\alpha}{N}EV\Delta t - \alpha E\Delta t - \Psi_2 E\Delta t$$

$$E(t+\Delta t) - E(t) = (\frac{\beta\alpha}{N}EV - \alpha E - \Psi_2 E)\Delta t$$

$$\frac{E(t+\Delta t) - E(t)}{\Delta t} = \frac{\beta\alpha}{N}EV - \alpha E - \Psi_2 E$$

$$\frac{\Delta E}{\Delta t} = \frac{\beta\alpha}{N}EV - \alpha E - \Psi_2 E$$

$$\lim_{\Delta t\to 0}\frac{\Delta E}{\Delta t} = \lim_{\Delta t\to 0}\frac{\beta\alpha}{N}EV - \alpha E - \Psi_2 E$$

$$\frac{dE}{dt} = \frac{\beta\alpha}{N}EV - \alpha E - \Psi_2 E$$

So the state transition rate at exposed state is

$$\frac{dE}{dt} = \frac{\beta\alpha}{N}EV - (\alpha + \Psi_2)E \qquad (2)$$

Transition process at infected state

Suppose that at time t the number of infected computers is $I(t)$ and at the time $(t + \Delta t)$ the number of vulnerable computers is $I(t + \Delta t)$. So the state transition rate from exposed state to infected state at the time Δt is $\alpha E \Delta t$, the state transition rate from infected state to secured state at the time Δt is $\gamma I \Delta t$. The process of number of change in infected state per unit time is as follows,

$$I(t + \Delta t) = I(t) + \alpha E \Delta t - \gamma I \Delta t$$

$$I(t + \Delta t) - I(t) = \alpha E \Delta t - \gamma I \Delta t$$

$$I(t + \Delta t) - I(t) = (\alpha E - \gamma I)\Delta t$$

$$\frac{I(t + \Delta t) - I(t)}{\Delta t} = \alpha E - \gamma I$$

$$\frac{\Delta I}{\Delta t} = \alpha E - \gamma I$$

$$\lim_{\Delta t \to 0} \frac{\Delta I}{\Delta t} = \lim_{\Delta t \to 0} \alpha E - \gamma I$$

$$\frac{dI}{dt} = \alpha E - \gamma I$$

So the state transition rate at exposed state is

$$\frac{dI}{dt} = \alpha E - \gamma I \quad (3)$$

Transition process at secured state

Suppose that at time t the number of infected computers is $S(t)$ and at the time $(t + \Delta t)$ the number of vulnerable computers is $S(t + \Delta t)$. So the State transition rate from vulnerable state to secured state at the time Δt is $\Psi_1 V \Delta t$, state transition rate from exposed state to secured state at the time Δt is $\Psi_2 E \Delta t$, state transition rate from infected state to secured state at the time Δt is $\gamma I \Delta t$ and the state transition rate from secured state to vulnerable state at the time Δt is $\phi S \Delta t$. The process of number of change in secured state per unit time is as follows

$$S(t + \Delta t) = S(t) + \Psi_1 V \Delta t + \Psi_2 E \Delta t + \gamma I \Delta t - \phi S \Delta t$$

$$S(t + \Delta t) - S(t) = \Psi_1 V \Delta t + \Psi_2 E \Delta t + \gamma I \Delta t - \phi S \Delta t$$

$$S(t + \Delta t) - S(t) = (\Psi_1 V + \Psi_2 E + \gamma I - \phi S)\Delta t$$

$$\frac{S(t+\Delta t) - S(t)}{\Delta t} = \Psi_1 V + \Psi_2 E + \gamma I - \phi S$$

$$\frac{\Delta S}{\Delta t} = \Psi_1 V + \Psi_2 E + \gamma I - \phi S$$

$$\lim_{\Delta t \to 0} \frac{\Delta S}{\Delta t} = \lim_{\Delta t \to 0} \Psi_1 V + \Psi_2 E + \gamma I - \phi S$$

$$\frac{dS}{dt} = \Psi_1 V + \Psi_2 E + \gamma I - \phi S$$

So the state transition rate at secured state is

$$\frac{dS}{dt} = \Psi_1 V + \Psi_2 E + \gamma I - \phi S \quad (4)$$

From Eq. (1), (2), (3) and (4) based on the transition process, the worm propagation model is:

$$\frac{dV}{dt} = -\frac{\beta \alpha}{N} EV - \Psi_1 V + \phi S \quad (5)$$

$$\frac{dE}{dt} = \frac{\beta \alpha}{N} EV - (\alpha + \Psi_2)E$$

$$\frac{dI}{dt} = \alpha E - \gamma I$$

$$\frac{dS}{dt} = \Psi_1 V + \Psi_2 E + \gamma I - \phi S$$

Assumed the total number of computers in a network is constant, then N = V (t) + E (t) + I (t) + S (t), which means that S (t) = N-V (t) -E (t) - I (t). So the model in Eq. (5) becomes,

$$\frac{dV}{dt} = \phi N - \frac{\beta \alpha}{N} EV - (\Psi_1 + \phi)V - \phi E - \phi I \quad (6)$$

$$\frac{dE}{dt} = \frac{\beta \alpha}{N} EV - (\alpha + \Psi_2)E$$

$$\frac{dI}{dt} = \alpha E - \gamma I$$

Equilibrium Points

Based on system of differential equation Eq. (6), two equilibrium points were obtained as

3.1 Worm free equilibrium points

Worm free equilibrium points mean all computers in the network are free from worm so $E = 0$ and from system of differential equation Eq. (6) the worm free equilibrium points occurs at $EQ_{wf} = (V_1^*, E_1^*, I_1^*) = (\frac{\phi}{(\Psi_1 + \phi)} N, 0, 0)$.

ISSN: 978-602-71169-7-9

Worm epidemic equilibrium points

Worm epidemic equilibrium points mean there is infected computer by worm and it can infected a new computer thus there is a worm propagation so E ≠ 0, and from system of differential equation Eq. (6) the worm epidemic equilibrium points occurs at $EQ_{we} = (V_2^*, E_2^*, I_2^*) =$
$(\frac{\alpha+\Psi_2}{\beta\alpha}N, \frac{\left(\phi-(\Psi_1+\phi)\frac{(\alpha+\Psi_2)}{\beta\alpha}\right)}{\left((\alpha+\Psi_2)+\phi+\phi\frac{\alpha}{\gamma}\right)}N, \frac{\alpha}{\gamma}E_2^*)$

Basic Reproduction Number

Basic reproduction number (R_0) is an average number of new computer on vulnerable computer state that infected by worm due to the influence of computer that already infected. If $R_0 < 1$, then every infected computer can only spread the infection to a new computer with an avarege less than one computer which mean there is no worm propagation. If $R_0 > 1$, then every infected computer can spread the infection to a new computer with an average more than one computer which mean there is worm propagation. Next Generation Matrix were used to obtain the basic reproduction number and here is the basic reproduction number:

$$R_0 = \frac{\beta\alpha\phi}{(\Psi_1+\phi)(\alpha+\Psi_2)} = 4.8076$$

Stability Analysis

5.1 Stability analysis on worm free equilibrium points

To analyze the stability of mathematic model of worm propagation on worm free equilibrium point, linearization system of the model were done by using the gradient method, according to the linearization, the jacobian matrix at worm free equilibrium points is:

$$J_{Q_{wf}} = \begin{bmatrix} -(\Psi_1+\phi) & -\frac{\beta\alpha}{N}\frac{\phi}{(\Psi_1+\phi)}N - \phi & -\phi \\ 0 & \frac{\beta\alpha}{N}\frac{\phi}{(\Psi_1+\phi)}N - (\alpha+\Psi_2) & 0 \\ 0 & \alpha & -\gamma \end{bmatrix}$$

The eigen value from jacobian matrix at free equilibrium points were obtained as follow:

$$\lambda_1 = -(\Psi_1+\phi)$$

$$\lambda_2 = \frac{\beta\alpha}{N}\frac{\phi}{(\Psi_1+\phi)}N - (\alpha+\Psi_2)$$

$$\lambda_3 = -\gamma$$

Equilibrium points is stable when the eigen value $\lambda_i = 0$, for $i = 1,2,3$ and equilibrium points is locally asymptotically stable when the eigen value $\lambda_i < 0$, for $i = 1,2,3$. Since all the parameter of the model have positive value, then $\lambda_1 < 0$ and $\lambda_3 < 0$, in order the equilibrium points is locally asymptotically stable then λ_2 has to less than 0, so the following condition has to be satisfied:

$$\frac{\beta\alpha}{N}\frac{\phi}{(\Psi_1+\phi)}N - (\alpha+\Psi_2) < 0$$

Lemma 1.

The worm free equilibrium EQ_{wf} is locally asymptotically stable when $R_0 \leq 1$ and the EQ_{wf} is unstable when $R_0 > 1$.

Proof 1.

To satisfied the condition for system to be asymptotically stable is that all eigenvalue has to be negative value. The stability condition satisfied if $\lambda_i < 0$ for i=1,2,3. Since the parameters Ψ_1, ϕ and γ has positive value so λ_1 and λ_3 has a negative value, λ_2 need to have a negative value too to satisfied the condition, so:

$$\frac{\beta\alpha}{N}\frac{\phi}{(\Psi_1+\phi)}N - (\alpha+\Psi_2) < 0$$

$$\frac{\phi}{(\Psi_1+\phi)}N < \frac{(\alpha+\Psi_2)}{\frac{\beta\alpha}{N}}$$

$$\frac{\beta\alpha\phi}{(\Psi_1+\phi)(\alpha+\Psi_2)} < 1$$

Because $R_0 < 1$, which is sufficient to the condition on lemma 1. Therefore the condition for system to be asymptotically stable are satisfied.

5.2 Stability analysis on worm epidemic equilibrium points

To analyze the stability of mathematic model of worm propagation on worm epidemic equilibrium point, linearization system of the model were done by using the gradient

method, according to the linearization, the jacobian matrix at worm epidemic equilibrium points is:

$$J_{EQ_{we}} = \begin{bmatrix} -\frac{\beta\alpha}{N}\frac{p}{q}N - (\Psi_1 + \phi) & -\alpha - \Psi_2 - \phi & -\phi \\ \frac{\beta\alpha}{N}\frac{p}{q}N & 0 & 0 \\ 0 & \alpha & -\gamma \end{bmatrix}$$

with $p = \phi - (\Psi_1 + \phi)\frac{(\alpha+\Psi_2)}{\beta\alpha}$ and $q = (\alpha + \Psi_2) + \phi + \phi\frac{\alpha}{\gamma}$

the characteristic polynomial at λ is:

$$h(\lambda) = a_3\lambda^3 + a_2\lambda^2 + a_1\lambda + a_0,$$

with

$$a_3 = 1$$

$$a_2 = \frac{\beta\alpha}{N}E_2^* + \Psi_1 + \phi + \gamma$$

$$a_1 = \left(\frac{\beta\alpha}{N}E_2^* + \Psi_1 + \phi\right)(\gamma) + \frac{\beta\alpha}{N}E_2^*(\alpha + \Psi_2 + \phi)$$

$$a_0 = \left(\frac{\beta\alpha}{N}E_2^*(\alpha + \Psi_2 + \phi)\right)\gamma + \frac{\beta\alpha}{N}E_2^*\alpha\phi$$

Stability analyze of worm epidemic equilibrium points determine by using Routh-Hurwitz criteria. Based on Routh-Hurwitz criteria, verifying that $\frac{a_1a_2 - a_0a_3}{a_2}$ has the same sign with a_1 , because all the parameter has a positive value. thus $a_0 > 0, a_1 > 0, a_2 > 0, a_3 > 0, \frac{a_1a_2 - a_0a_3}{a_2} > 0$ and $a_1a_2 > a_0a_3$ so the Routh-Hurwitz stability criteria are satisfied, hence all the eigen value has a negative value. So the worm epidemic equilibrium is locally asymptotically stable.

Case Study

Numerical simulation for this mathematic model used the method of Runge-Kutta fourth Order, using the data from Computer Laboratory, Mathematics Department of Faculty of Sciences and Mathematics, Diponegoro University for initial value and without prejudice to the generality parameter values based on the literature [8], the simulation conducted with MATLAB and through the simulation we will find out the worm propagation in every state and the model stability.

Two equilibrium points were obtained as:

Worm free equilibrium points

From substituted the parameter value to the Eq.(6) Worm free equilibrium points were obtained as:

$$(V_1^*, E_1^*, I_1^*) = \left(\frac{\phi}{(\Psi_1+\phi)}N, 0, 0\right) = (15, 0, 0)$$

The eigenvalue of jacobian matrix on worm free equilibrium points are -0.0008, 11.75025 and 0.5 because not all eigenvalue have a negative value thus the model not stable at worm free equilibrium so there is a worm propagation on a network

Worm endemic equilibrium points

From substituted the parameter value to the Eq.(6) Worm endemic equilibrium points were obtained as:

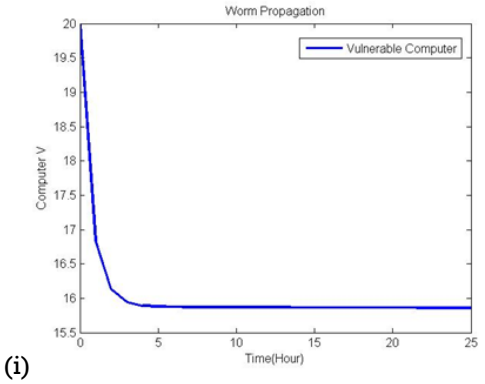
$$(V_2^*, E_2^*, I_2^*) = \left(\frac{\alpha+\Psi_2}{\beta\alpha}N, \frac{\left(\phi - (\Psi_1+\phi)\frac{(\alpha+\Psi_2)}{\beta\alpha}\right)}{\left((\alpha+\Psi_2) + \phi + \phi\frac{\alpha}{\gamma}\right)}N, \frac{\alpha}{\gamma}E_2^*\right) = (3.12006, 0.00176, 0.00307)$$

The eigenvalue of jacobian matrix on endemic equilibrium points -3.086, -0.5 and -0.0038 because all eigenvalue have a negative value thus the model locally asymptotically stable at worm endemic equilibrium points so there is a worm propagation on a network.

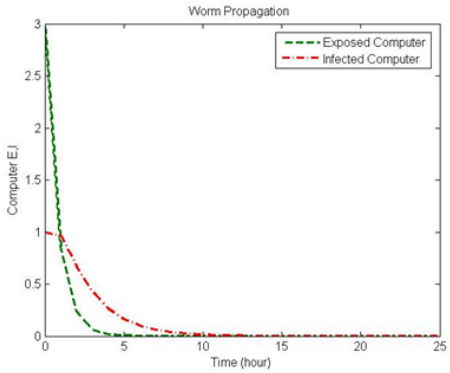
Basic reproduction number were obtained from the parameter value is $R_0 = 4.8076 > 1$, which mean every infected computer can spread the infection to a new computer with an average more than one computer then there is worm propagation.

Here is the results number of change of computer in every state using MATLAB:

ISSN: 978-602-71169-7-9



(i)



(2)

Figure 1. (1) The number of change of computer in vulnerable state **(2)** The number of change of computer in exposed and infected state

Fig.(1) show that computer in vulnerable state prone to have a reduction which mean the number of vulnerable computers will decreased by every hour. Fig. (2) show that computer in exposed and infected state prone to have a reduction which mean the number of exposed and infected computers will decreased by every hour.

Conclusion

Based on the result of mathematic model of worm propagation two equilibrium points were obtain, worm free equilibrium points = $\left(\frac{\phi}{(\Psi_1+\phi)}N, 0, 0\right) = (15, 0, 0)$ and worm epidemic equilibrium points = $\left(\frac{\alpha+\Psi_2}{\beta\alpha}N, \frac{\left(\phi-(\Psi_1+\phi)\frac{(\alpha+\Psi_2)}{\beta\alpha}\right)}{\left((\alpha+\Psi_2)+\phi+\phi\frac{\alpha}{\gamma}\right)}N, \frac{\alpha}{\gamma}E_2^*\right)$.

From the simulation result using MATLAB, worm propagation and the number of change of computer in every state were obtained as computer in vulnerable state prone to have a reduction and computer in exposed and infected state also prone to have a reduction. The stability analysis for endemic equilibrium is stable locally asymptotic which mean there is a worm propagation in a network.

Reference

[1] Nazario, Jose. 2004. Defense and Detection Strategies against Internet Worms. Artech House

[2] A.Friedman, Good neighbors can make good fences: a peer-to-peer use security system, IEE Technol, Soc, Magaz, 26 (1) (2007) 17-24

[3] D.Moore, V.Paxson, S,Savage, C. Shannon, S. Staniford, N. Weaver, Inside the Slammer worm, IEEE Magaz, Secur, Privacy 1 (4) (2003) 33-39

[4] D. Moore, C. Shannon, J. Brown, Code red: a Case Study on the Spread and Victims of an Internet Worm, in: Proceedings of the 2nd ACM SIGCOMM Workshop on Internet Measurement, Marseille, France, Nov. 2002, pp. 273–284.

[5] Dressler, J. (2007). "United States v. Morris". Cases and Materials on Criminal Law. St. Paul, MN: Thomson/West. ISBN 978-0-314-17719-3

[6] Li P, Salour M, Su X. A survey of internet worm detection and containment. IEEE Communications Surveys and Tutorials, 2008, 10(1): 20–35

[7] M.R. Faghani, H. Saidi, Social networks' XSS worms, in: Proceedings of the International Conference Computational Science and Engineering, CSE '09, vol. 4, 29–31 Aug. 2009, pp. 1137–1141.

[8] Toutonji, Ossama A. Seong-Moo Y. Moongyu P. 2012. Stability Analysis of VEISV Propagation Modelling for Network Worm Attack. Applied Mathematic Modelling. Vol 36. Hal 2751-2761

[9] Mishra, B. M. dan Pandey S. K. (2010). Fuzzy Epidemic Model for the Transmission of Worms in Computer Network, Nonliear Analysis: Real World Applications, 11, hal. 4335-4341.

[10] J. Kim, S. Radhakrishana, J. Jang, Cost optimization in SIS model of worm infection, ETRI J. 28 (5) (2006) 692–695.