Stability analysis of VEISV propagation modeling for network worm attack

Ossama A. Toutonji, Seong-Moo Yoo, Moongyu Park

Electrical and Computer Engineering Department, The University of Alabama in Huntsville, USA
Department of Mathematical Science, The University of Alabama in Huntsville, USA

In this paper, we propose VEISV (vulnerable – exposed – infectious – secured – vulnerable) network worm attack model, which is appropriate for measuring the effects of security countermeasures on worm propagation. Contrary to existing models, our model takes into consideration accurate positions for dysfunctional hosts and their replacements in state transition. Using the reproduction rate, we derive global stability of a worm-free state and local stability of a unique worm-epidemic state. Furthermore, simulation results show the positive impact of increasing security countermeasures in the vulnerable state on worm-exposed and infectious propagation waves. Finally, equilibrium points are confirmed by phase plots.

1. Introduction

Worm attacks are considered by network experts the highest security risk on computer network security, functionality and assets. Attackers use a malicious worm as a primary tool to target software vulnerabilities. Computer worms are built to propagate without warning or user interaction, causing an increase in network traffic service requests that will eventually lead to distributed denial-of-service (DDoS). However, recent worm assaults exceeded common impacts such as DDoS or backdoor listener and caused financial losses and threatened the security of classified information.

On November 2, 1988, Robert Morris launched the first network worm named Morris. The payload was designed to target DEC machines with virtual address extension running 4BSD and Sun3 operating systems, and was intended to gauge the size of the Internet. The Morris worm was capable of infecting an estimated 60,000 computers, costing approximately $100 million in damages [1]. On July 13, 2001, two network administrators, both employees of eEye Digital Security Company, discovered the Code Red worm, which targeted Microsoft internet information services web servers (MS-IIS). The worm was capable of infecting the same machine multiple times and simultaneously used a random number generator seed to create a list of IP addresses to scan on port 80/TCP. The attack severely caused DDoS, infected 360,000 hosts, and caused $2.6 billion in financial losses [2–4,1]. On January 25, 2003, the Slammer worm began to propagate by exploiting buffer-overflow vulnerability in Internet-connected computers running Microsoft relation model database server MS-SQL. The Slammer infected approximately 75,000 hosts and achieved a full scanning rate of 55 million scans per second which caused network outages [1,5]. The Conficker worm launched on November 21, 2008, and was able to pass through nearly every Windows 2K and XP honeypot, infecting over 13 million IP addresses throughout the world-wide network [6–11]. The payload in the worm is built from a combination of malicious malware whose capabilities exceed the common malicious worm impairment.
To fight malicious worms, ethical worms were developed. On August 18, 2003, W32-Welchia, an ethical worm, was released to exploit vulnerabilities in Microsoft XP Remote Procedure Call (RPC) by using TCP port 135 and the WebDav vulnerability by using TCP port 80 running MS IIS 5.0. Even though the intention of launching an ethical worm is clearly to do no harm, network security officers still oppose the use of any type of computer worm in general. There are indications that even ethical worms, like their malicious counterparts, will increase network traffic, reboot infected computers, and operate without the consent of users.[12]

Recently, there exists much research in the literature as overviewed in Section 2 in this paper. So far, there is no way to prevent the worm propagation in a short period immediately after detecting the worm. Thus, current research focuses on mitigating the propagation speed and modeling the propagation accurately considering the network stability.

The novel idea in the proposed model is to consider security countermeasures. They are involved in preventing, detecting, and defending against worm attacks in various states of the model. The countermeasure’s effects are also analyzed on the exposed and the infectious wave.

In this paper, we propose VEISV (vulnerable – exposed – infectious – secured – vulnerable) network worm attack model, which is appropriate for measuring the effects of security countermeasures on worm propagation. Contrary to existing models, our model takes into consideration accurate positions for dysfunctional hosts and their replacements in state transition. Using the reproduction rate, we derive global stability of a worm-free state and local stability of a unique worm-epidemic state. Furthermore, simulation results show the positive impact of increasing security countermeasures in the vulnerable state on worm-exposed and infectious propagation waves. Finally, equilibrium points are confirmed by phase plots.

This paper organized as follows: Section 2 overviews related work. Section 3 describes the proposed model, the model’s assumptions, and the set of differential equations. Section 4 presents the stability analysis[13–15] of the proposed model. Section 5 covers the numerical analysis and the simulation. Section 6 concludes the paper.

2. Related work

The similarity between the spread of a biological virus and malicious worm propagation encourages researchers to adopt an epidemic model to the network environment[16]. Research in modeling computer viruses and worms implement epidemic models like SIR[17–19], SIS[16], SEIR[20–25,13], SIRS[26,27], and SEIQV[28]. The purpose is to study worm propagation by developing different transaction states based on the behavior of the virus or the worm. This section summarizes research topics in the areas of modeling malicious worms, modeling benign worms, quarantine defense mechanism, and stability analysis.

2.1. Stability analysis

Li and Zhen[21] studied the global asymptotical stability of the SEI epidemic model with general contact rate. The global asymptotical stability and the disease-free equilibrium were examined by using the Lyapunov function, LaSalle’s invariant set theorem and Poincare–Bendixson property. Mishra and Zha[22,23] investigated the fixed period of temporary immunity after running anti-malicious software on computer nodes and modeling a malicious object in a computer network by using the SEIQRS model. Their results, supported by numerical analysis, showed that the threshold value of the reproduction rate determines the outcome of the diseases. Yi et al.[24] presented detailed analysis of the SEIR dynamic system by considering variable parameters with seasonal forcing in the transmission rate. Furthermore, in the case of one varying parameter, the periodic, chaotic, and hyperchaotic dynamical behaviors are investigated by using the bifurcation diagrams, Lyapunov exponent spectrum diagram and Poincare section. Sun et al.[25] developed the contact rate threshold for a SEIR epidemic model using nonlinear incidence rates, constant recruitment and disease-caused death. The results revealed the condition that the disease-free equilibrium is globally stable. Yuan and Chen[13] developed a mathematical model for network virus point-to-group information propagation. The new e-SEIR model considered three network factors including multi-state antivirus, latent period between exposed and infectious states, and point-to-group information propagation mode. Furthermore, theoretical investigations had been done on several related dynamics properties and equilibrium stability.

2.2. Malicious worms, benign worms, and quarantine defense

In Zou et al.[30] modeled and analyzed Code Red worm propagation based on the two-factor Kermack–Mckendrick epidemic model. The numerical analysis led to better understanding and prediction of the scale and speed of the spreading Internet worm. Chen et al.[31] presented the Analytical Active Worm Propagation (AAWP) model for Code Red, which characterizes the propagation of worms that employ local subnet random scanning. The research includes a comparison between the AAWP model, the epidemiological model, and Weaver’s simulator as well as a quantitative analysis of worm detection. Yang et al.[32] presented the dynamic model of file diffusion in peer to peer (P2P) file-sharing networks. The study discussed the following three types of P2P states: peers in idle states, peers in exposed states, and peers in the state of downloading. Zhou et al.[19] analyzed extensively the positive effects (passive, active and hybrid) of ethical worms against the spread of malicious worms based on two-factor epidemic model. Moore et al.[33] developed the Internet quarantine requirements for containing self-propagating code by using three key parameters: reaction time, containment strategy and deployment sce-
The final results showed significant administrative gaps to be bridged before an effective defense could be provided against network worm attacks. Wang et al. [28] presented stability analysis of a SEIQV epidemic model for rapid spreading worms. The study considered quarantine and vaccination as the two main recovery countermeasures. Furthermore, the reproduction rate for the SEIQV model was developed to analyze model stability. Furthermore, Burckhardt [34] proposed a virtual reality modeling of infectious diseases in the human population. The model considered two important factors, the level of contact between individuals and the duration of immunity in the graveyard stage. Burckhardt’s research suggested new ways to reduce widespread infection by using quarantine and treatment in human population as a future study.

Kim and Bentley [33] explored the similarity between the human immune system and network intrusion detection systems and studied the possibility of emulating the human immune system to design a novel network-based intrusion detection system.

3. VEISV worm attack propagation model

Yuan and Chen [13] proposed e-SEIR network virus-epidemic model. The model extended the SEIR (susceptible – exposed – infectious – recovered) model to study the spread of computer network viruses. Here, they took into consideration three network environment factors; multi-state antivirus, latent period before the infected host becomes infectious, and point-to-group information propagation mode. They also made the analysis of how to control computer network virus prevalence based on the equilibrium stability.

We argue that the e-SIRS modeling technique is more proper to analyze computer worm than computer virus since the worm is propagated across computer networks but the virus is not [10]. In addition, there are many arguable claims in the e-SEIR model.

The SEIR epidemic model is characterized by a fixed latent period between the exposed and the infectious states for the virus to be active and propagate. In a conventional computer virus, propagation does not occur without user interaction, which results in an indeterminate value for the latent period. Network multi-malware worms like Conficker spread through the network without user interaction with an average latent time of 3.5 h, making the SEIR model suitable for computer worm modeling [13,10].

The e-SEIR model adopted the concepts of birth and death, where replacements occur in susceptible state, and dysfunction occur in all susceptible, exposed, infectious, and recovered states. Since this concept does not fit with a real network environment, we notice two problematical issues. First, during the worm attack, the dysfunction of network hosts occurs only in the infectious state. Second, the replacement of dysfunctional hosts does not occur in the susceptible state. These arguments motivate us to propose a more suitable VEISV model.

To develop the VEISV model we took into account information terminology and security countermeasures that have been used to prevent and defend against worm attacks. Thus, we use the state name vulnerable instead of susceptible and secured instead of recovered. The state transitions of hosts in the VEISV model is summarized as follows: vulnerable $\rightarrow$ exposed $\rightarrow$ infectious $\rightarrow$ secured $\rightarrow$ vulnerable.

The vulnerable state includes all hosts which are vulnerable to worm attack. Exposed state includes all hosts which are exposed to attack but not actively infectious due to the latent time requirement. Infectious state includes all hosts which

---

**Fig. 1.** The VEISV model.
were attacked and actively scanning and targeting new victims. Secured state includes all hosts which gained one or more security countermeasures, providing the host with a temporary or permanent immunity against the malicious worm.

In the newly proposed VEISV model, the following was observed: first, during a worm attack, hosts’ dysfunction occurred in the infectious state whereby the hosts are taken over by a worm and are not capable of performing properly; second, the hosts replaced during the attack are fully up-to-date with security measures, having been replaced in the secured state.

Fig. 1 shows in detail a block diagram of the VEISV model state transition and model parameters involved. Table 1 shows notation used in this paper and initial parameter values to be used in Section 5. The data sources of the initial values are mentioned in the section. Table 2 shows a summary of the state transitions and rates of hosts in the VEISV model.

Differing from previous virus or worm modeling research, the VEISV model took into consideration the security countermeasures involved in preventing and defending against worm attack, and the effect of adjusting the security countermeasures on the exposed and the infectious wave. As shown in Fig. 1, the recovery routes for V, E, and I state to estimate the recovery rate for each state in a real network worm attack. From the recovery routes, we considered security countermeasures as follows: (1) The recovery route in the vulnerable state (V–S) was derived from the security countermeasures (SCs) taken in the V state to prevent the attack. (2) The recovery route in exposed state (E–S) was derived from the SCs taken in the E state after detecting the attack. (3) The recovery route in the infective state (I–S) was derived from the SCs taken in state I after the worm became active. (4) Hosts that gained temporary immunity status in the secured state could lose immunity and move back to the vulnerable state causing infectious outbreaks.

From Fig. 1, the host’s state progresses as follows: vulnerable hosts exposed to the worm transitioned to the exposed state. After a latent period, the hosts move to the infectious state in which the worm begins actively scanning the network for new victims. A portion of vulnerable and exposed hosts in the network, with sufficient security countermeasures, will avoid the attack and move to the secured state.

Hosts in the infectious state, in which a security patch or update have been installed, move to the secured state. Hosts in the secured state, which lose immunity, will move back to the vulnerable state. The replacement and dysfunctional hosts are represented respectively by S and I states.

We built the VEISV model based on the following assumptions:

(1) The total number of hosts $N$ is fixed and defined in Eq. (1):

$$ N = V(t) + E(t) + I(t) + S(t). $$

(2) Initially, all hosts are vulnerable to attack. The total number of quarantined hosts, without considering the quarantine time, will move to the secure state after installing the required security patches or updates.

(3) The number of replaced hosts is equal to the number of dysfunctional hosts and the model is a closed network defined:

<table>
<thead>
<tr>
<th>Table 1</th>
<th>Notation and parameters values for the VEISV model.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Notation</td>
<td>Explanation</td>
</tr>
<tr>
<td>$V(t)$</td>
<td>Number of vulnerable hosts at time $t$</td>
</tr>
<tr>
<td>$E(t)$</td>
<td>Number of exposed hosts at time $t$</td>
</tr>
<tr>
<td>$I(t)$</td>
<td>Number of infectious hosts at time $t$</td>
</tr>
<tr>
<td>$S(t)$</td>
<td>Number of secured hosts at time $t$</td>
</tr>
<tr>
<td>$\beta$</td>
<td>Contact rate</td>
</tr>
<tr>
<td>$\gamma$</td>
<td>State transition rate from E to I</td>
</tr>
<tr>
<td>$\phi_1$</td>
<td>State transition rate from V to S</td>
</tr>
<tr>
<td>$\phi_2$</td>
<td>State transition rate from E to S</td>
</tr>
<tr>
<td>$\gamma$</td>
<td>State transition rate from I to S</td>
</tr>
<tr>
<td>$\phi$</td>
<td>State transition rate from S to V</td>
</tr>
<tr>
<td>$N$</td>
<td>Total number of hosts</td>
</tr>
<tr>
<td>$\theta$</td>
<td>Dysfunctional rate</td>
</tr>
<tr>
<td>$\mu$</td>
<td>Replacement rate</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Table 2</th>
<th>State transition events and transition rates.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Events include intermediate security measures</td>
<td>Rate of transition</td>
</tr>
<tr>
<td>$V \rightarrow E$</td>
<td>$\beta V(t)$</td>
</tr>
<tr>
<td>$V \rightarrow S$</td>
<td>$\phi_1 V(t)$</td>
</tr>
<tr>
<td>$E \rightarrow I$</td>
<td>$\gamma E(t)$</td>
</tr>
<tr>
<td>$E \rightarrow S$</td>
<td>$\phi_2 E(t)$</td>
</tr>
<tr>
<td>$I \rightarrow S$</td>
<td>$\gamma I(t)$</td>
</tr>
<tr>
<td>$I$</td>
<td>Dysfunctional</td>
</tr>
<tr>
<td>Replaced $\rightarrow S$</td>
<td>$\mu N$</td>
</tr>
</tbody>
</table>
\[\Gamma = \{(V, E, I, S) \in \mathbb{R}^4 \mid V + E + I + S = N\}. \tag{2}\]

Since the number of hosts is large, we defined the incident of infection as \(\beta \frac{V(t)}{N}I(t)\). \(\beta\) represents the number of incidents occurring in a unit of time. The transition of hosts from the \(V\) state to \(E\) state in terms of \(\Delta t\) is:
\[\Delta VE = \beta \frac{V(t)}{N}I(t)\Delta t. \tag{3}\]

Since \(\alpha E(t)\) is the number of attacked hosts moved to the infectious state, we define the force of incident \(f\):
\[f = \frac{\beta \alpha}{N}. \tag{4}\]

We can evaluate the number of transitioning vulnerable hosts from time \(t\) to \((t + \Delta t)\) by the following equation:
\[V(t + \Delta t) - V(t) = -fE(t)V(t)\Delta t - \psi_1 V(t)\Delta t + \phi S(t). \tag{5}\]

We followed the mathematical approach in [35] to derive the theoretical part. This set of differential equations governs the VEISV model:
\[
\begin{align*}
\frac{dV}{dt} &= -fEV - \psi_1 V + \phi S, \\
\frac{dE}{dt} &= fEV - (\alpha + \psi_2)E, \\
\frac{dI}{dt} &= \alpha E - (\gamma + \theta)I, \\
\frac{dS}{dt} &= \mu N + \psi_1 V + \psi_2 E + \gamma I - \phi S.
\end{align*}
\tag{6}\]

4. Stability analysis VEISV model

Since, \(S(t) = N - V(t) - E(t) - I(t)\), we can use the reduction method by considering only the first three equations of (6) to analyze our model
\[
\begin{align*}
\frac{dV}{dt} &= \phi N - fEV - (\psi_1 + \phi)V - \phi E - \phi I, \\
\frac{dE}{dt} &= fEV - (\alpha + \psi_2)E, \\
\frac{dI}{dt} &= \alpha E - (\gamma + \theta)I.
\end{align*}
\tag{7}\]

To study the stability of model (7), first, we must find the equilibrium points at steady states of the VEISV model which satisfy the following equations:
\[
\begin{align*}
\frac{dV}{dt} &= 0, \\
\frac{dE}{dt} &= 0, \\
\frac{dI}{dt} &= 0.
\end{align*}
\tag{8}\]

For \(dE(t)/dt = 0\), the equilibrium occurs at:
\[E^* = 0 \text{ or } E^* > 0 \text{ and } V^* = \frac{\alpha + \psi_2}{\beta \alpha} N. \tag{9}\]

For \(E^* = 0\), the worm-free equilibrium occurs at:
\[EQ_{w0} = (V_1^*, E_1^*, I_1^*) = \left(\frac{\phi}{\psi_1 + \phi} N, 0, 0\right). \tag{10}\]

For \(E^* > 0\), the worm-epidemic equilibrium is:
\[EQ_{we} = (V_2^*, E_2^*, I_2^*) = \left(\frac{\alpha + \psi_2}{\beta \alpha} N, \frac{\phi - (\frac{\alpha + \psi_2}{\beta \alpha})(\psi_1 - \phi)}{\alpha + \psi_2 + \phi \left(1 + \frac{\alpha}{\gamma + \theta}\right)} N, \frac{\alpha}{\gamma + \theta} E_2\right). \tag{11}\]

4.1. Stability of worm-free state

According to Eqs. (6) and (10), the Jacobian matrix at the point \(EQ_{w0}\) is:
\[J(EQ_{w0}) = \begin{pmatrix}
-(\psi_1 + \phi) & -(\psi_1 + \phi) & -\phi \\
0 & fV_1 - (\alpha + \psi_2) & 0 \\
0 & \alpha & -((\gamma + \theta))
\end{pmatrix}. \tag{12}\]

The corresponding eigenvalues of \(J(EQ_{w0})\) are:
\[
\begin{align*}
\lambda_1 &= - (\psi + \phi), \\
\lambda_2 &= fV_1 - (\alpha + \psi_2), \\
\lambda_3 &= - (\gamma + \phi) .
\end{align*}
\] (13)

Because all parameters of the model have positive real values, \( \lambda_1 < 0, \lambda_3 < 0 \), for a worm-free equilibrium to be locally asymptotically stable, the following condition has to be satisfied:

\[
fV_1 - (\alpha + \psi_2) < 0.
\] (14)

To define the basic reproduction number of infections, we see that it is meaningful only if \( E_2 > 0 \), it is easy to show the denominator of \( E_2 \) in Eq. (11), i.e.

\[
\alpha + \psi_2 + \phi \left( 1 + \frac{\alpha}{f} + \theta \right) > 0.
\] (15)

Since all parameters are positive values, we just need to show that the numerator >0:

\[
\phi - \frac{\alpha + \psi_2}{\beta^2} (\psi_1 + \phi) > 0.
\] (16)

From Eq. (16), we conclude that the reproduction rate:

\[
R_0 = \frac{\alpha \beta \phi}{(\psi_1 + \phi)(\alpha + \psi_2)}.
\] (17)

For the previous conclusions we can develop the following Lemmas regarding the stability of the worm-free equilibrium.

**Lemma 1.** Based on the definition of \( R_0 \) in Eq. (17), 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.** By stability theorem in [14], the sufficient condition for the three dimensional system to be asymptotically stable is that all eigenvalues are negative values. The stability condition is satisfied if \( \lambda_i < 0 \), for \( i = 1, 2, 3 \). It is easy to show that \( \lambda_1 < 0 \), and \( \lambda_3 < 0 \), for VEISV system. As to \( \lambda_2, \lambda_2 < 0 \) is equivalent to

\[
V_1 < (\alpha + \psi_2)/f.
\] (18)

By substituting \( V_1 = \phi N/(\psi_1 + \phi) \) and \( f = \alpha \beta /N \) into Eq. (18), we have \( \frac{\alpha \beta \phi}{(\psi_1 + \phi)(\alpha + \psi_2)} < 1 \), which is the sufficient condition in the lemma. \( \square \)

**Theorem 1.** The worm-free state is globally asymptotically stable if \( R_0 \leq 1 \).

**Proof 2.** Learn from the first equation of system (7)

\[
V'(t) \leq \phi N - (\psi + \phi)V(t).
\]

Thus

\[
V(t) \leq \frac{\phi N}{\psi_1 + \phi} + (V(0) - \frac{\phi N}{\psi_1 + \phi}) \exp[-(\psi_1 + \phi)t].
\]

When \( t \to \infty \), we obtain

\[
V(t) \leq \frac{\phi N}{\psi_1 + \phi}.
\]

Let us consider the following Lyapunov function defined by \( L(t) = E(t) \). The time derivative of \( L(t) \) is

\[
L'(t) = E'(t) = \frac{\phi N}{\psi_1 + \phi} V(t) - (\alpha + \psi_2)E(t) \leq \frac{\phi N}{\psi_1 + \phi} E(t) - (\alpha + \psi_2)E(t) = (\alpha + \psi_2)E(t) \left[ \frac{\alpha \beta \phi}{(\psi_1 + \phi)(\alpha + \psi_2)} - 1 \right] \leq 0.
\]

So we prove that the worm-free equilibrium \( J(EQ_{wf}) \) is globally stable. \( \square \)

4.2. Stability of worm-epidemic state

For the case of worm-epidemic state, the Jacobian matrix at \( EQ_{we} \) is:
The characteristic polynomial of $J(\mathbf{Q}_{\omega\psi})$ is:

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

where

\[
\begin{align*}
\begin{cases}
  a_1 = 1, \\
  a_2 = (\gamma + \theta) + (\alpha + \psi_2) + (\mathbf{E}_2^2 + \psi_1 + \phi), \\
  a_1 = (\gamma + \theta)(\alpha + \psi_2 + \mathbf{E}_2^2 + \psi_1 + \phi) + (\alpha + \psi_2)(\mathbf{E}_2^2 + \psi_1 + \phi) + \phi\mathbf{E}_2^2, \\
  a_0 = (\gamma + \theta)(\alpha + \psi_2)(\mathbf{E}_2^2 + \psi_1 + \phi) + \phi\mathbf{E}_2^2 + \phi\mathbf{E}_2^2.
\end{cases}
\end{align*}
\]

Lemma 2. Worm-epidemic state is locally asymptotically stable if $R_0 > 1$.

Proof 3. By the Routh–Hurwitz criterion [36], the Routh–Hurwitz Array for $J(\mathbf{Q}_{\omega\psi})$ is as follows:

\[
\begin{bmatrix}
  a_3 & a_1 \\
  a_2 & a_0 \\
  (a_1 a_2 - a_0 a_3) / a_2 & 0 \\
  a_0 & 0
\end{bmatrix}.
\]

Based on Routh–Hurwitz conditions [36], verifying that $(a_1 a_2 - a_0 a_3) / a_2$ has the same sign with $a_1$, then the three eigenvalues have negative real parts. Since $a_0 > 0$, $a_1 > 0$, $a_2 > 0$, $a_3 > 0$, $(a_1 a_2 - a_0 a_3) / a_2 > 0$ and $a_1 a_2 > a_0 a_3$ hold. Therefore, the Routh–Hurwitz stability conditions are satisfied, and the worm-epidemic equilibrium is locally asymptotically stable. □

4.3. Worm-epidemic control

Similar analysis of reproduction rate in Theorem 1 highlights the efforts needed to prevent the widespread of worm through network.

Corollary 1. To stop the worm’s propagation, the recovery rate in V-state should satisfy

$$\psi_1 > \phi \left( \frac{\beta\alpha}{\alpha + \psi_2} - 1 \right).$$

Proof 4. From both Eq. (17) and Theorem 1, this corollary holds. □

The proposed model is more realistic compared to existing worm propagation models. First, the security countermeasures are considered contrary to existing models. Second, the concepts of birth and death are applied more properly, i.e. a death occurs only in the infectious state and a birth occurs in the secured state after fully updated with security measures.

Next, we will compare our proposed model to existing propagation models in terms of stability. Refer to Table 3. The stability of our proposed model is close to those of existing models.

5. Numerical analysis

In this section, we developed experimental steps to serve mainly in analyzing the stability of the proposed model and evaluating the effects of the implemented security countermeasures.

<table>
<thead>
<tr>
<th></th>
<th>[23]</th>
<th>[13]</th>
<th>[28]</th>
<th>Proposed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Worm-free Local</td>
<td>$R_0 &lt; 1$</td>
<td>$R_0 &lt; 1$</td>
<td>$R_0 &lt; 1$</td>
<td>$R_0 &lt; 1$</td>
</tr>
<tr>
<td>Worm-free Global</td>
<td>$R_0 \leq 1$</td>
<td>$R_0 \leq 1$</td>
<td>$R_0 \leq 1$</td>
<td>$R_0 \leq 1$</td>
</tr>
<tr>
<td>Worm-epidemic Local</td>
<td>$R_0 &gt; 1$</td>
<td>$R_0 &gt; 1$</td>
<td>$R_0 &gt; 1$</td>
<td>$R_0 &gt; 1$</td>
</tr>
<tr>
<td>Worm-epidemic Global</td>
<td>$R_0 &gt; 1$</td>
<td>$R_0 &gt; 1$</td>
<td>$R_0 &gt; 1$</td>
<td>$R_0 &gt; 1$</td>
</tr>
</tbody>
</table>
It is very hard to use some real-world worm traffic traces or realistic parameters for research. Even traffic traces used in research papers (e.g. Slammer [1] and Code-red [37]) are not public. From the published papers [1,37] we are not able to find parameters that can be used in our model. Generally, when the available traces are too small or sampled, they can be inappropriate to perform a careful traffic analysis. Most available traces from CAIDA (www.caida.org) or MIT do not contain the rest of the legitimate traffic flow on links since the traces were deliberately filtered before making them available. This does not allow us to find proper parameters between the worm traffic and the legitimate traffic flow on the same link at the same time. However, we have tried to select parameters from Conficker worm explained in next two paragraphs.

Refer to Tables 1 and 2. The initial parameter values were calculated and chosen carefully to better suit a real multi-malware worm attack scenario. In 2009, Panda Security, an antivirus vendor, used active scanning to gauge the number of hosts infected by the Conficker worm. The study showed that only 6% of attacked hosts in the USA were infected [38]. Furthermore, considering the worm’s dormant time, we estimated the average latent time of the Conficker worm to be 3.5 h, during which time, the worm will perform the following tasks: checking the Windows version, copying the malicious library to the system root directory under a random file name, checking the firewall to open backdoor listeners, and activating randomly generated IP addresses. An infected host scans 250 domain names every 3 h [30]. Table 2 shows notation and parameter values.

To find the model’s parameters, both an experimental and reverse solution method were used. Technical reports about the Conficker attack gave an estimated value of the number of (V,I) hosts. The simulation time was 2–2.5 months. The total number of hosts was \((14 \times 10^5)\) in which all were initially vulnerable to attack. The maximum rate of infection was 6%. In the exposed state, hosts were still able to connect to the Internet, perform a scan for worm detection and download security updates. The average time for exposed hosts to recover in this experiment was 20 min. The latent time for infectious hosts was set accordingly to achieve 6% maximum infection. In network recovery processes from multi-malware worm attacks, studies showed that the number of vulnerable hosts that recovered from the attack was small due to the lack of passive security countermeasures which should have been taken initially to prevent the attack [19].

To measure the impact of the worm attack in a real network environment, the recovery rate was set for the vulnerable state to \(\psi_1 = 0.0003\). Furthermore, the state transition from S to V was set as: \(\phi = 0.0005\).

Fig. 2. Worm propagation \((V,S)\) for \(E(0) = 10\) and \(R_0 = 2.62\).

Fig. 3. Worm propagation \((E,I)\) for \(E(0) = 10\) and \(R_0 = 2.62\).
Fig. 2 shows the system behavior when initial values of exposed and infectious hosts were set respectively at $E(0) = 10$, $I(0) = 1$. With an approximately calculated value of $R_0 = 2.62$, the result showed multiple outbreaks in the worm infection that eventually reached an epidemic stability without control for equilibrium points. Figs. 2 and 3 show the network behavior without control for $E/C^3 > 0$; $I/C^3 > 0$.

From Eq. (17), increasing the security countermeasures in the V-state decreased the reproduction rate that brought the network to stability in a shorter period. Our results showed the disappearance of infection outbreaks and a noticeable decline in both the exposed and the infectious waves. Figs. 4 and 5 show the VEISV model simulation output for $R_0 < 1$.

Finally, Figs. 6 and 7 show the phase plots for V–S–I states and S–I–E states, respectively, which confirm the local stability for $R_0 = 2.62$. 
6. Conclusion

Due to the latent time between the susceptible and the infectious state, the e-SEIR epidemic model is more suitable for modeling a multi-malware network worm attack than a computer virus. By using network security terminology, we renamed the SEIR epidemic states and defined the locations for dysfunctional hosts and their replacements that enabled us to identify the secure routes for our new VEISV model. Mathematically, we developed the reproduction rate from the generated set of differential equations for the VEISV model. The simulation results, supported by the theoretical approach showed that all worms were able to pervade if the reproduction rate is greater than one, and the worm epidemic died out when the rate is smaller than one. Furthermore, we discussed the level of immunity required in the vulnerable state which helped to overcome the spread of the worm throughout the network. We are currently under research how to prevent the worm propagation immediately after detecting the worm attack.

References


