Scan-Based Worms: The Impact of IPV4 Address Space on Epidemic Computer Network Models

ChukwuNonso H. Nwokoye *Member, IAENG*, Ikechukwu I. Umeh, Njideka N. Mbeledogu, and Vincent O. S. Okeke

***Abstract* – The propagation of malicious codes such as worms have been characterized using compartmental epidemic models which are mostly mathematical equations. Aside the challenge of identifying the type of virus or worm represented by these compartmental models, we noticed that the representation of internet protocol (IP) address space is absent. Therefore, this study evaluates the impact of the IPV4 address space using the following epidemic models; SAIR, SEIR, SEI-V, SEIQR and Q-SEIR. By our modifications, the implication is that these models now characterize the scan-based worms that probe the address space in order to find and attack vulnerable computers. To the best of our knowledge, this is the first study that evaluates the impact of this IP addressing format on epidemic computer network models. Numerical simulations with the Runge-Kutta order 4 and 5 method are used to illustrate several existent variations with the models without IPV4 address space. Results are time histories and 3 dimensional phase plots of the models, and from them it was discovered that the standard incidence cancels the effect of adding the expression of IPV4 address scanning space for the worms. More so, characteristically temporal variations were also noted for the susceptible compartment of these models.**

***Index Terms*–Computer Network, Worms, IPV4, Epidemic Model, Differential Equations.**

I. Introduction

In these days of connected systems and computers, malicious codes such as worms and their variants have become a perpetual source of harm and security risk to individuals and organizations that operate using the ubiquitous internet. These worms render information and communication technology (ICT) infrastructure momentarily unreachable, cause enormous losses, disrupt social activities and is regarded as a weapon of cyber warfare. As Wang, *et al.* [1] puts it, “a computer worm is a program that self-propagates across a network exploiting security or policy flaws in widely-used services”. Examples of sophisticated worms that has wrecked mayhem include Code Red worm, Blaster worm, Conficker worm, Stuxnet. The connected nature of the computers, most especially on the internet, implies that every system is potentially at risk of worm attack. To curb these catastrophes caused by worms, researches have invested huge finances into developing anti-malicious software that provide immunity for computer systems. However, with the continual appearances of worm variants, the immunity offered by anti-malware can only be ephemeral and short-lived. On worm categorization using target-search process, Wang, *et al.* [1] posited that worms are classified into scan-based worms and topology-based worms. Our interest in this study is the former. They also maintained that, “scan-based worms (scanning worms) propagates by probing the entire IPv4 space or a set of IP addresses and directly compromises vulnerable target hosts without human interference” [1]. Scanning strategies include random and localized scanning.

Aside containment and security approaches that involve anti-malware and firewall [2], mathematical models are used to provide insights into complex epidemic problems in the network through simulation experiments that describe the dynamical behavior of agents in a networked environment. This approach has been widely applied in public health where the infectious outcomes of a disease-causing agent are assessed so as to gain understanding of spread patterns and other containment approaches. Due to the connective similarities between viruses in biological networks [3, 4] and malwares in telecommunication networks [5], researchers have applied compartment models to wireless sensor [6–13] and computer networks so as to achieve diverse ends. Additionally, network researchers have represented transfer of infections from servers to client nodes as well as other scenarios and phenomena that occur in a real world network. In recent times, mathematical models have addressed the following issues; malicious code spread [14, 15], isolation and treatment of virus/worm infection [16, 17], inoculation [18, 19], infection latency [20], fuzziness [21], effect of anti-malicious code software [22, 23] and e-vaccine application on susceptible nodes [24, 25].

The addressing requirements of a network is a phenomena that hasn’t been extensively studied using the epidemic models. Though, Song, *et al* [26] modelled address space, there is need to elicit its impact in an extensive study using other computer network models. The network layer of the Transmission Control Protocol/Internet Protocol (TCP/IP) suite houses the two popular types of address spaces, they include the IP version 4 (IPV4) and IP version 6 (IPV6). The network layer solves the issue of internetworking by handling the responsibility of packet transmission from source to destination. IPV4 is a 32-bit addressing format that has 2^{32} addresses i.e. 4.294.967.296 addresses. On the other hand, IPV6 is 128-bit addressing format that has 2^{128} addresses i.e. $3.4*10^{38}$ addresses. Some notable differences exist between the two formats. These differences are in the following area; addressing and routing, security, network address translation, administrative workload, and support for mobile devices [27].

The paper is structured as follows; Section II is the review of pertinent literature while Section III contains the methodology

Manuscript received July 14, 2020; revised December 21, 2020

C. H. Nwokoye is a Researcher of National Open University of Nigeria Unit of the Nigerian Correctional Service, Anambra State Command (phone: +2347033858720; e-mail: chinonsonwokoye@gmail.com)

I. I. Umeh is a Lecturer of Computer Science Department, Faculty of Physical Sciences, Nnamdi Azikiwe University, Nigeria (email: ikumeh@gmail.com)

N. N. Mbeledogu is a Senior Lecturer of Computer Science Department, Faculty of Physical Sciences, Nnamdi Azikiwe University, Nigeria (e-mail: njideembeledoguu@yahoo.com)

V. O. S. Okeke is a Senior Lecturer with Chukwuemeka Odumegwu Ojukwu University, Anambra, Nigeria (e-mail: explode2kg@yahoo.com)

used for the study. Section IV presents the SIRM$_S$M$_I$ model and the simulation for the impact of IPV4. This provided the rationale for modifying six computer network models contained in Section IV. Section V presents the conclusions and future directions.

II. Related Works

Here, we reviewed some computer network epidemic models that litter the extant literature on network epidemiology. It is noteworthy that even though these models represent worm attacks in a computer networks, none of them represented the internet protocol address space that are probed to discover vulnerabilities. The following are the reviewed models. Investigating the use of classical epidemiological models for studying computer virus propagation, Piqueira, *et al*. [28] modified the Susceptible-Infected-Removed (SIR) epidemiological models so as to introduce the anti-viral compartment (SIRA) and analysed the stability of the disease free equilibrium points.

Mishra and Saini [29] formulated an epidemic transmission model (SEIRS) of malicious objects in the computer network. Therein they assumed that the death rate of computers other than attack of malicious object is constant. The model consists of a set of integro-differential equations. When a node is recovered from the infected class, it recovers temporarily, acquiring transient immunity with probability P (O≤P≤I) and dies from the attack of malicious object with probability (I - p). Mishra and Saini [30] developed four mathematical models on computer viruses infecting the system under different conditions. SIRS epidemic model was developed by Mishra and Jha [31] with a fixed period of temporary immunity, following temporary recovery from the infection of malicious objects in place of an exponentially distributed period of temporary immunity.

Yuan and Chen [32] proposed a new network virus epidemic model which they called the e-SIER. This is unlike other existing computer virus propagation models because it takes into consideration three, important network environment factors which include (1) multi-state antivirus, (2) latent periods before the infected hosts become infectious and (3) point to group information propagation mode. Piqueira and Ceasar [33] developed a dynamic model for virus propagation. Here, classical epidemiological models for disease propagation are adapted to computer networks and, by using simple systems identification techniques a model called SAIC (Susceptible, Antidotal, Infectious, and Contaminated) was developed. Real data about computer viruses are used to validate the model i.e. Comparisons between model outputs and real data presented shows that the model can be considered adequate to describe the spreading evolution of a computer virus.

In the work of Piqueira and Araujo [34], a modified version of the Susceptible-Infected-Removed (SIR) model was presented like Piqueira and Ceasar [33] and how its parameters are related to network characteristics were explained. The modification here is by allowing the inclusion of a block that represents the antidotal population, thereby generating a SAIR (Susceptible-Antidotal-Infected-Removed). Compared to the SIR model, the antidotal population therein represents some machines in the network equipped with anti-virus programs. Mishra and Nayak [35] proposed a Susceptible (S)–Infectious (I) epidemic model for active infectious nodes in computer sub-networks where nodes continuously interact with each other. Here, the Infectious compartment is divided into active infectious and non-active infectious nodes.

Saini [36] presented a different perspective to infection modeling by proposing and analysing a nonlinear mathematical model (PIM) to study the effect of malicious object on the immune response of the computer network. Mishra and Pandey [19] formulated an e-epidemic SEIRS model for the transmission of worms in computer network through vertical transmission. The stability of the result was stated in terms of modified reproductive number.

Mishra and Kumar [37] formulated a Susceptible(S)-Infectious (I) model for transmission of worms in Computer network. The SIS model for the infective periods of fixed length due to the attack of computer worms gave rise to the formulation of three different epidemic models. The effect of time delay on infected nodes was analysed which also includes worms transmission in vertical ways on the nodes of the computer network.

The model in Mishra and Pandey [19] is similar to Mishra and Pandey [38] but differ in the sense that an attempt was made (in the latter) to mathematically formulate a compartmental Susceptible–Exposed–Infectious–Susceptible with Vaccination (SEIS–V) epidemic transmission model of worms in a computer network with natural death rate, which depends on the total number of nodes. Additionally, they analysed their contribution of vertical transmission to the modified reproductive number as well as the performance analysis of efficient antivirus software. Numerical methods were employed to solve and simulate the system of equations developed and interpretation of the model yielded interesting revelations. Kumara, *et al.* [39] developed a compartmental e-Epidemic Susceptible-Infectious-Highly Infectious-Recovered (SIJR) model of viruses in a computer network with natural death (that is, crashing of nodes due to the reason other than the attack of viruses). The infectious class here changes infectivity i.e. the progression from less infectious to highly infectious stage.

III. Methodology

To actualize the study, we modified some epidemic computer network models by adding the expression for IPV4 addressing configuration. The implication is that the resulting compartmental models now represents scan-based worms that search the IP address space for weaknesses. The differential equation models, posed like an initial value problem requires a numerical method in order to provide solutions [40], therefore, the Runge-Kutta order 4 and 5 (RK45) numerical method was used for this purpose [41]. Numerical simulations was done in order to generate time histories and three dimensional (3D) phase plots which are used to highlight the impact of IP addressing configurations in computer networks containing scan-based worms. During these simulation experiments, the parametric values of the original epidemic models were adapted.

III. IPv4 Address Space and Epidemic Models

Of great importance is the model proposed by Song, *et al* [26] to address web scanning and removable external devices. This model comprises of five compartments namely; susceptible (*S*), infected (*I*), immunized (*R*), susceptible media (M_S) and infected media (M_I). The SIRM$_S$M$_I$ model has the IPv4 address protocol, where 2^{32} represents the size of the scanning space and the chance of discovering a vulnerable computer in one scan, denoted as $S/2^{32}$. Note that the assumptions of the original model is maintained here. The SIRM$_S$M$_I$ is given as system (1) below:

$$\begin{aligned} \dot{S} &= b_1 - \frac{\beta_1 SI}{2^{32}} - \frac{\beta_2 SM_1}{S+I+R} - \mu_1 S \\ \dot{I} &= \frac{\beta_1 SI}{2^{32}} - \frac{\beta_2 SM_1}{S+I+R} - \delta_1 S - \mu_1 I \\ \dot{R} &= \delta_1 I - \mu_1 R \\ \dot{M}_S &= b_2 - \frac{\beta_2 M_S I}{S+I+R} + \delta_2 M_1 - \mu_2 M_S \\ \dot{M}_I &= \frac{\beta_2 M_S I}{S+I+R} - \delta_2 M_I - \mu_2 M_I \end{aligned} \tag{1}$$

Using the RK45 method, we performed the numerical simulation experiments to show the behaviour of the compartments. The experiments depicted the impact of the addition and removal of the expression for IPv4 scan space at rates; β_1= 0.042 and β_2= 0.024, which are the infection rates of computers and infected media respectively. Other values used for the simulations include μ_1, μ_2 ((obsolescence rate of computers and the obsolescence rate of removable devices) = 0.0027 and δ_1 (recovery rates of infected computers) = 0.033, δ_2 (recovery rates of infected media) = 0.0082. During the simulation, the initial values of the compartments were 200, 70, 20, 10, 10 for S, I, R, M$_S$ and M$_I$ respectively.

Taking a close look at the two results that constitute Fig. 1 and Fig. 2, it is clear that they are different, thence, showing the impact of the IPv4 address space. The intersection of infectious and recovered compartments of the first result (Fig. 1) with IPv4 was at (13, 43) while the second result (Fig. 2) without IPv4 was at (19, 136) for (x, y) axes.

Investigating the dynamics of the network, more variations were succinctly and subsequently shown using Fig. 3 and Fig. 4, which is are 3D plots of the SIRM$_S$M$_I$ model. During that simulation, the infectivity rates were increased in this manner; β_1= 0.042, 0.046, 0.050 and β_2 = 0.024, 0.028, 0.032. Specifically, Fig. 3 is the 3D plot of the SIRM$_S$M$_I$ model with IPV4 representing the dynamics of Susceptible, Infected and Recovered compartments. While Fig. 4 is the 3D phase plot of the SIRM$_S$M$_I$ model without IPV4 showing the dynamics of Susceptible, Infected and Recovered compartments. For the latter, one can see that responses overlap, while for the former responses are slightly separated.

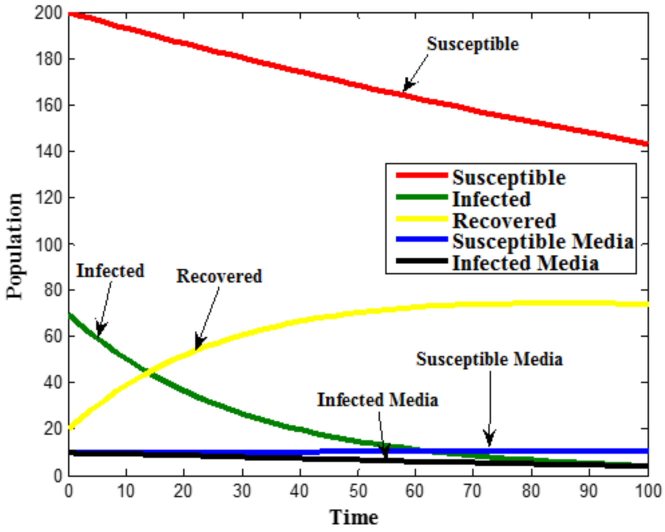

Fig. 1. SIRM$_S$M$_I$ model with IPv4

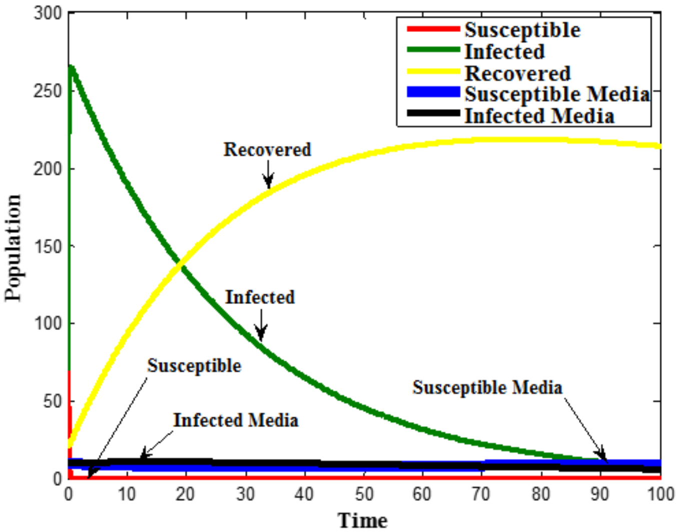

Fig. 2. SIRM$_S$M$_I$ model without IPv4

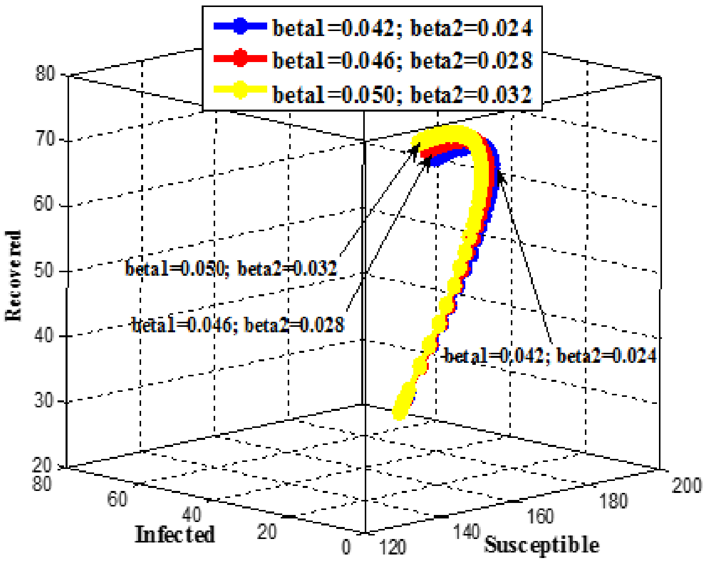

Fig. 3. 3D plot of the SIRM$_S$M$_I$ model with IPV4 for S, I, R compartments

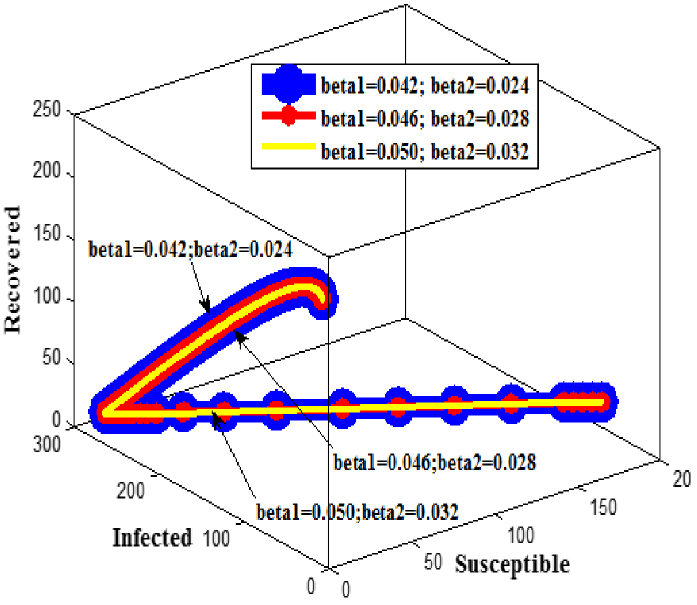

Fig. 4. 3D plot of the SIRM$_S$M$_I$ model without IPV4 for S, I, R compartments

To highlight the dynamics of the remaining compartments i.e. the Susceptible Media and Infected Media, we performed simulation experiments that gave rise to Fig. 5 and Fig. 6. These figures further showed the variations existent for the presence and absence of IPV4 addressing configuration in the SIRM$_S$M$_I$ epidemic model.

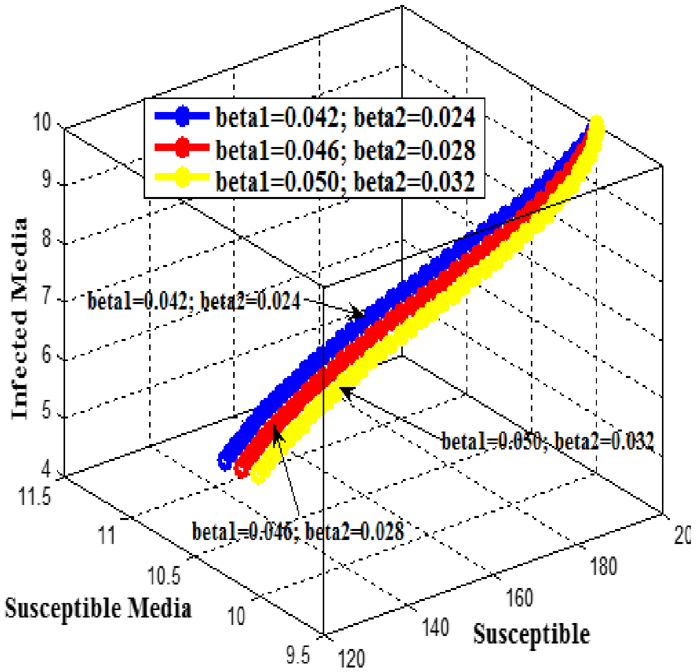

Fig. 5. 3D plot of the SIRM$_S$M$_I$ model with IPV4 for S, M$_S$, M$_I$ compartments

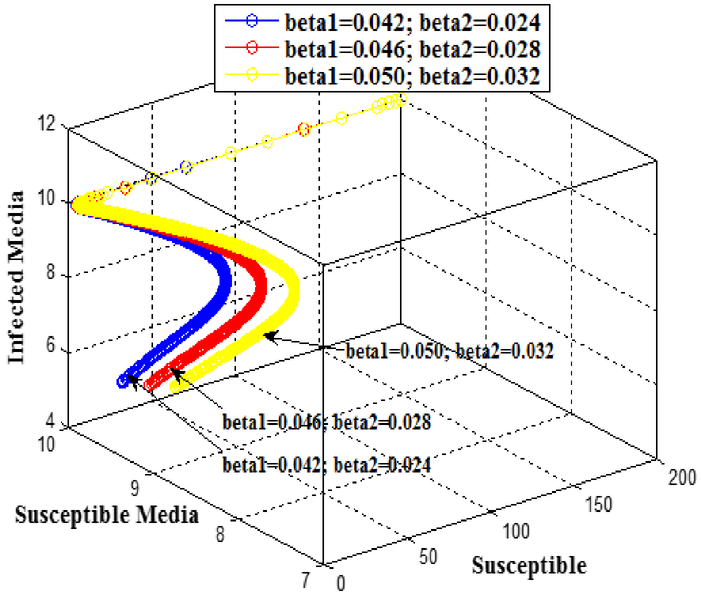

Fig. 6. 3D plot of the SIRM$_S$M$_I$ model without IPV4 for S, M$_S$, M$_I$ compartment

IV. Epidemic Models: Numerical Simulation

The epidemic computer network models to be evaluated were culled from the extant literature on network epidemiology. However, our study here is absent analysis on removable devices also represented in the above model of Song, *et al.* [26]. The analyses involving some selected modified computer network models are listed in the following subsections. Note that numerical simulations following model descriptions are performed using the RK45 numerical method.

A. The SAIR Model

The SAIR model was originally designed by Piqueira and Araujo [34] for virus propagation, but it can be applied to worm spread in computer networks. The population of computers *(T)* are divided into four compartments namely; the non-infective and vulnerable computers *(S)*, the antidotal computers *(A)* i.e. nodes equipped with anti-malicious software, the infective computers (*I*) and the removed computers (*R*) as a result of infection or otherwise. The assumptions of the model include *N*: addition of new computers to the network, μ: death rate due to worm infection, $\beta SI/2^{32}$: the effective infectious rate as a result of the worm probing the IPV4 address space in search of vulnerable nodes, α_1: equipping the susceptible computers with anti-malicious software, α_2: the conversion of infective computers to antidotal state, δ: the removal rate of unfixable computers, σ: the restoration and conversion of removed computer to the susceptible state. At $N = 0$ there is no addition of new computers and the four groups S+I+R+A equals the T. The SAIR is given as system (2) below:

$$\begin{aligned}
\dot{S} &= N - \alpha_1 S - \frac{\beta SI}{2^{32}} - \mu S - \sigma R \\
\dot{I} &= \frac{\beta SI}{2^{32}} - \alpha_2 I - \delta S - \mu I \qquad (2) \\
\dot{R} &= \delta I - \sigma R - \mu R \\
\dot{A} &= \alpha_1 S + \alpha_2 I - \mu A
\end{aligned}$$

Numerical simulations using the specified numerical method resulted in Fig. 7 and Fig. 8. The simulation experiments were done using the following values: N=100; α_1 = 0.025; α_2 = 0.25; β = 0.1; μ = 0.01; σ = 0.8; δ =20; while the initial values are S = 74; I = 25; R = 0, A = 1. The simulations shows that there is significant difference for the addition or otherwise of the expression of IPV4 address space. The four groups of S, A, I, R vary for addition of IPV4. The greatest difference is visible if one considers the R compartment; with address space representation (Fig. 7), R was persistently 0 alongside the infected compartment. Conversely, without IPV4 (Fig. 8) it was seen to rise to unimaginable points.

Investigating the dynamics of this network, the differences were clearly shown using Fig. 9 and Fig. 10, which are the 3D plots of the SAIR model. During that simulation, the infectivity rates were increased in this manner; β = 0.1, 0.5, 1.0. Specifically, Fig. 9 is the 3D plot of the SAIR model with IPV4 representing the dynamics of Susceptible, Infected and Recovered compartments. While Fig. 10 is the 3D plot of the SAIR model without IPV4 showing the dynamics of Susceptible, Infected and Recovered compartments.

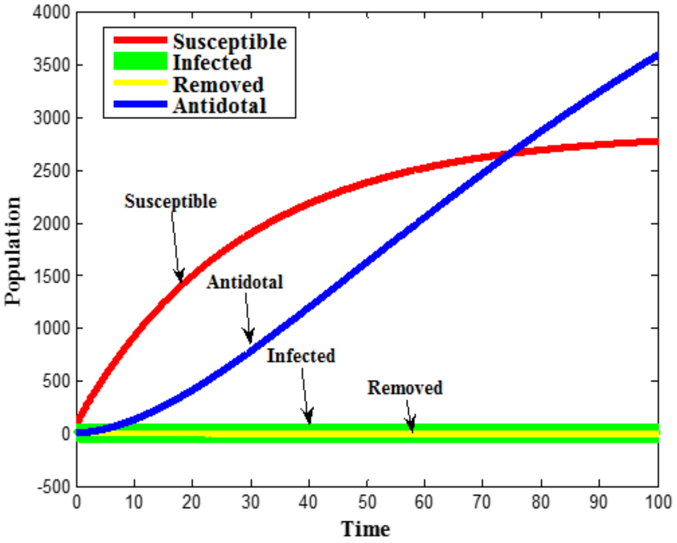

Fig. 7. SAIR model with IPv4

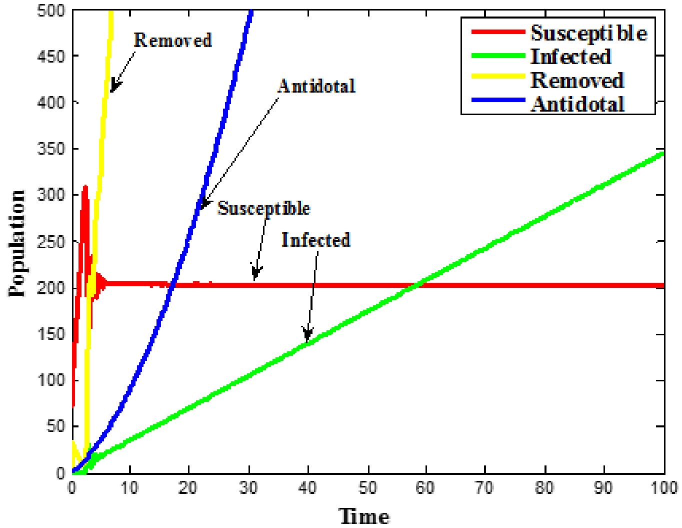

Fig. 8. SAIR model without IPv4

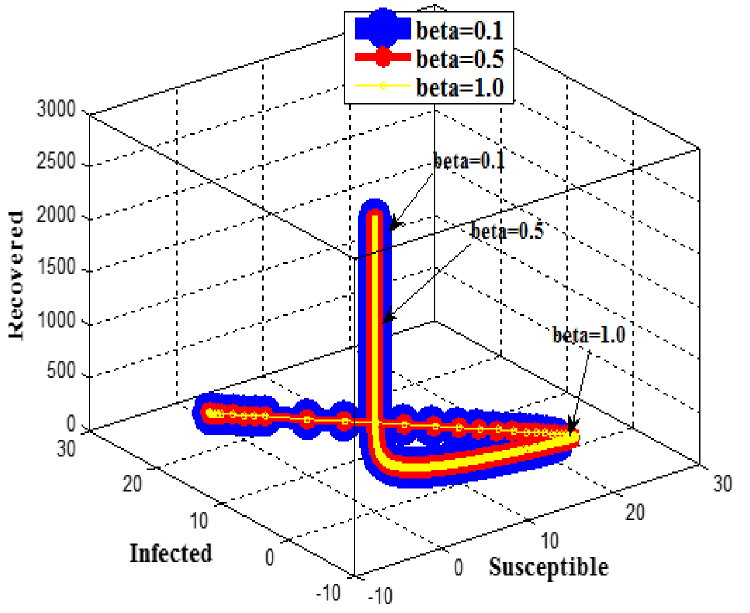

Fig 9. 3D plot of the SAIR model with IPV4 for S, I, R compartments

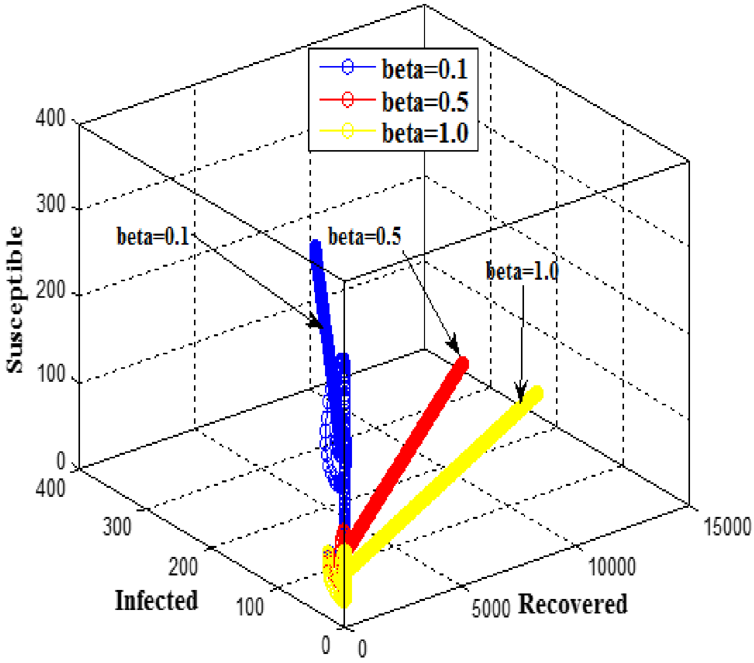

Fig 10. 3D plot of the SAIR model without IPV4 for S, I, R compartments

B. The SEIQRS Model

The SEIQRS model was originally proposed by Mishra and Jha [42]. Therein, the population of computers were divided into subgroups of susceptible, exposed, infectious, quarantined, and recovered, represented as $S(t)$, $E(t)$, $I(t)$, $Q(t)$, $R(t)$ respectively. The original assumptions of the model are retained alongside the expression of IPV4 address space. The parameters include; A: addition of new computers to the susceptible class, d: rate of death due to reasons other than the malicious code attack, μ: transition for exposed class to the infective class i.e. the computers become fully infectious, δ: rate at which infectious computers are isolated, α: the mortality rate as a result of worm infection, ε: recovery rate for quarantined computers, γ: recovery rate for infected computers, and η: immunity loss. The SEIQRS is given as system (3) below:

$$\begin{aligned} \dot{S} &= A - \frac{\beta SI}{2^{32}} - dS + \eta R \\ \dot{E} &= \frac{\beta SI}{2^{32}} - (d + \mu)E \\ \dot{I} &= \mu E - (d + \alpha + \gamma + \delta)I \\ \dot{Q} &= \delta I - (d + \alpha + \varepsilon)Q \\ \dot{R} &= \gamma I + \varepsilon Q - (d + \eta)R \end{aligned} \qquad (3)$$

Numerical simulations of the SEIQRS model using the specified numerical method resulted in Fig. 5 and Fig. 6. The simulation experiments were done using the following values: A = 0.3, d = 0.1, μ = 0.3, β = 0.3, γ = 1.8, ε = 0.3, η = 0.2, α = 0.2, δ = 3.8. The initial values were using 200, 100, 50, 0, 0 for *S(t), E(t), I(t), Q(t), R(t)* respectively. The Exposed compartment (which contains computers who have contacted the infection but are not fully infectious) was above 250 when the time history was plotted without IPV4 address space (Fig. 11). Conversely, when IPV4 was involved in the simulation (Fig. 12), the E compartment was at 98 computers. Specifically, by analysing Fig. 12, it is obvious that the addition of IP addressing requirement to the SEIQRS model lowered the quarantine and recovery rates of computer nodes and changed the behaviour of the susceptible compartment.

Studying the dynamics of this network, the differences were clearly shown using Fig. 13 and Fig. 14, which are the 3D plots of the SEIQRS model. During that simulation, the infectivity rates were increased in this manner; β = 0.3, 0.8, 1.3. While Fig. 13 is the 3D plot of the SEIQRS model with IPV4 representing the dynamics of Susceptible, Exposed and Infected compartments. Fig. 14 is the 3D plot of the SEIQRS model without IPV4 showing the dynamics of Susceptible, Exposed and Infected compartments.

Using the same values of varying infectiousness, we sought to elicit the internal dynamics of Quarantined and Recovered compartments alongside the Susceptible compartment, and this is depicted as Fig. 15 and Fig. 16.

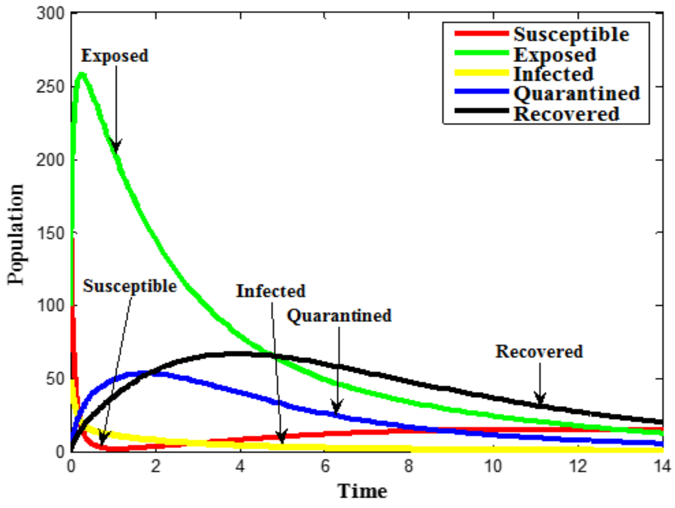

Fig. 11. SEIQRS model without IPv4

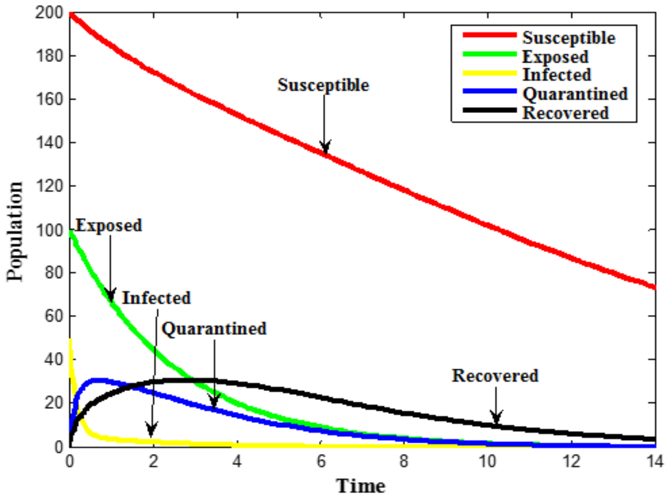

Fig. 12. SEIQRS model with IPV4

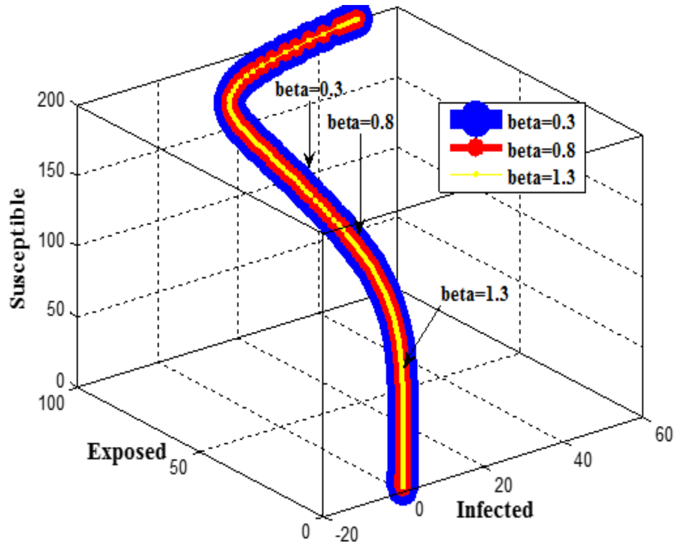

Fig. 13. 3D plot of the SEIQRS model with IPV4 for S, E, I compartments

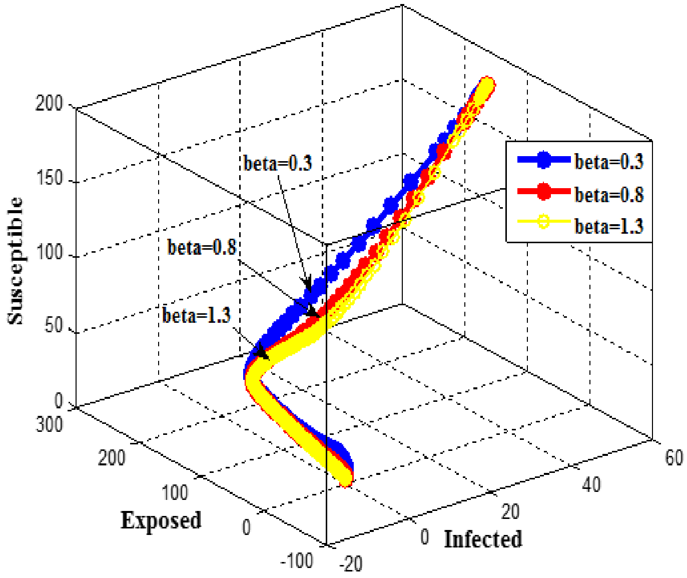

Fig. 14. 3D plot of the SEIQRS model without IPV4 for S, E, I compartments

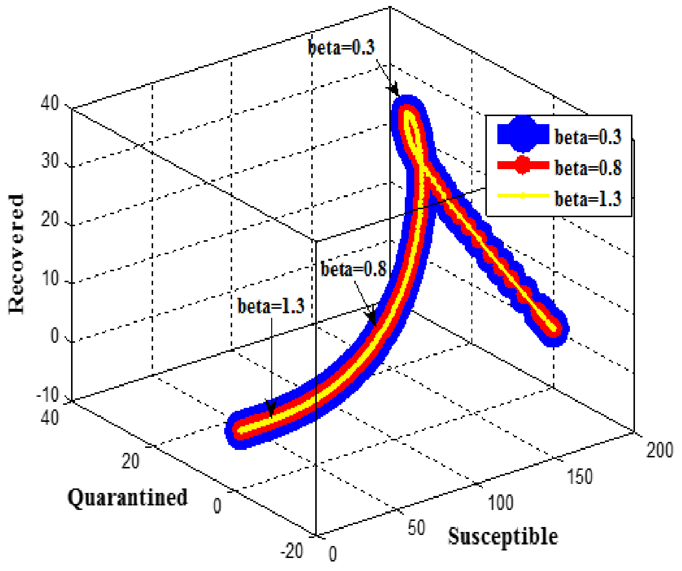

Fig. 15. 3D plot of the SEIQRS model with IPV4 for S, Q, R compartments

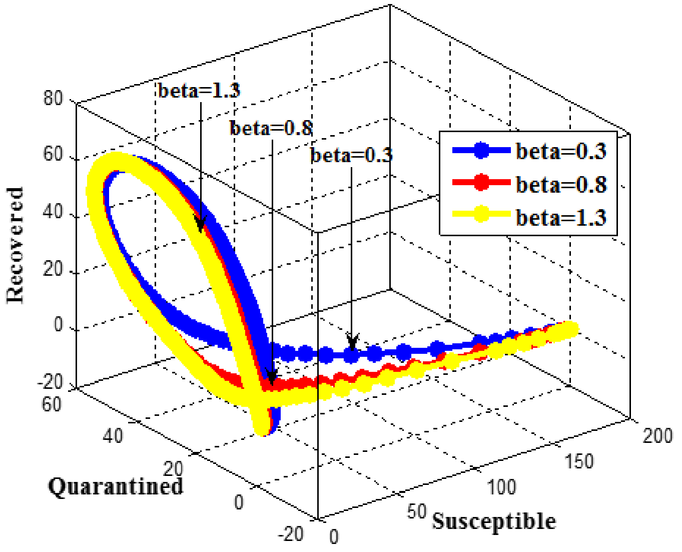

Fig. 16. 3D plot of the SEIQRS model without IPV4 for S, Q, R compartments

C. *The SEIR-S Vertical Transmission*

Here, the proponents [19] of the original SEIR-S Model, added vertical transmission (VT) alongside the ubiquitous horizontal malware transfers treated by most compartmental models of network epidemiology. Described as the transition from the main server to any of the client computers, VT hasn't been extensively addressed in epidemiology of computer networks. Alongside the following assumptions of the original model which was retained for this study, we add the expression for IPV4 address space for the scan-based worms as described. Note that with mass action as the chosen infection incidence, the effective infectious rate as a result of scan-based probes of the address space is given as $\lambda SI/2^{32}$.

The total population of computers N, are divided into *S(t), E(t), I(t)* and *R(t)* representing the susceptible, exposed (infected but not yet infectious), infectious and recovered, respectively. Other assumptions of the model include; *b*: the addition of new susceptible nodes to the network, *d*: death rate as a result of hardware failure or other reasons expect worm infection, ε: the transition from the *E* compartment to the *I* compartment, *η*: death rate as a result of worm infection, *γ*: transition between infectious compartment to the recovered compartment, ζ is the rate of re-infection after loss of immunity. On vertical transmission, it is assumed in the model that a portion *p* and a portion *q* of the new computers are added to the exposed compartment *E*. Therefore, the expression for this birth flux into compartment *E* is described as *pbE* + *qbI* while that of susceptible compartment is described as *b* – *pbE* – *qbI*. In the light of the above, the SEIR-S model is given as system (4) below:

$$\begin{aligned} \dot{S} &= b - \frac{\lambda SI}{2^{32}} - pbE - qbI - \delta S + \zeta R \\ \dot{E} &= \frac{\lambda SI}{2^{32}} + pbE + qbI - \varepsilon E - dE \\ \dot{I} &= \varepsilon E - \gamma I - dI - \eta I \\ \dot{R} &= \gamma I + \zeta R - dR \end{aligned} \qquad (4)$$

Numerical simulations of the SEIRS model using the specified numerical method resulted in Fig. 17 and Fig. 18. The simulation experiments were done using the following values: *b* = 1.2, *p* = 0.1, *q* = 0.15, *η* = 0.3, *d* = 0.2, *λ* = 1.3, *ε* = 0.4, *γ* = 0.6, *ζ* = 0.8. The initial values were 70, 30, 10, 0 for *S(t), E(t), I (t), R(t)* respectively. It is clear that there is a difference between the results. The Susceptible compartment started from the initial value and gradually attempts to reach 0 on the x axis for the inclusion of IPV4 (Fig. 17). On the hand, the Susceptible compartment dipped to 0 at once, for the absence of the IPV4 expression (Fig. 18). The Exposed and Infected compartments also shows variations.

Examining the dynamics of this model, the differences were clearly shown using Fig. 19 and Fig. 20, which are the 3D plots of the SEIR-S model. During this simulation, the infectious rates were varied in this manner; *λ* = 1.3, 1.8, 2.3. While Fig. 19 is the 3D plot of the SEIR-S model with IPV4 representing the dynamics of Susceptible, Exposed and Infected compartments. Fig. 20 is the 3D plot of the SEIR-S model without IPV4 showing the dynamics of Susceptible, Exposed and Infected compartments. The Recovered compartment was not included in the 3D simulations because its behavior were not so different if one considers Fig. 17 and Fig. 18.

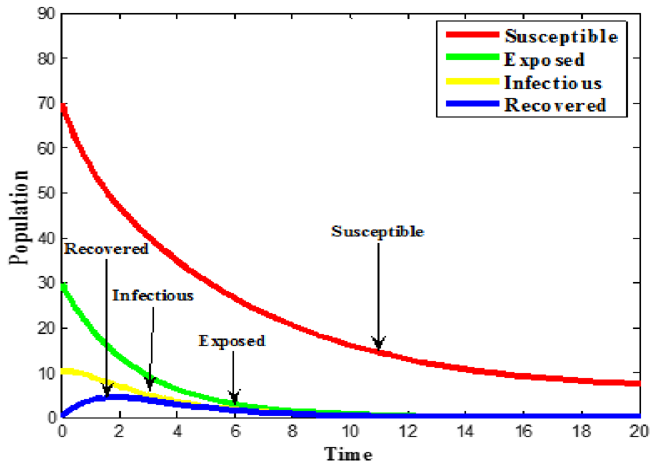

Fig. 17. SEIR model with IPV4

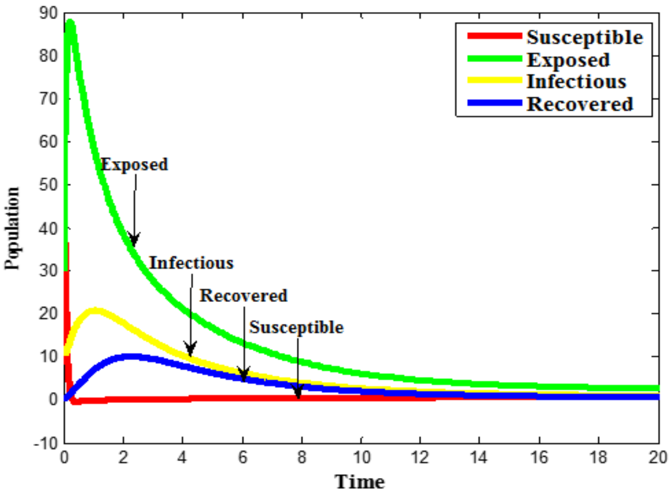

Fig. 18. SEIR model without IPV4

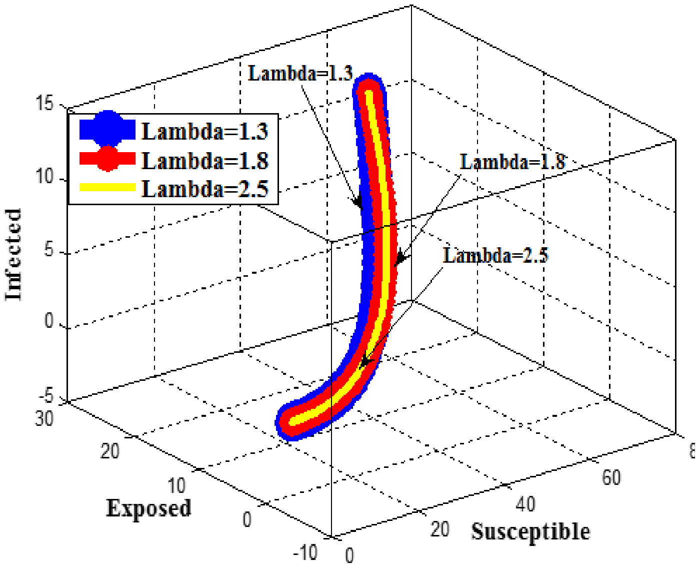

Fig. 19. 3D plot of the SEIR-S model with IPV4 for S, E, I compartments

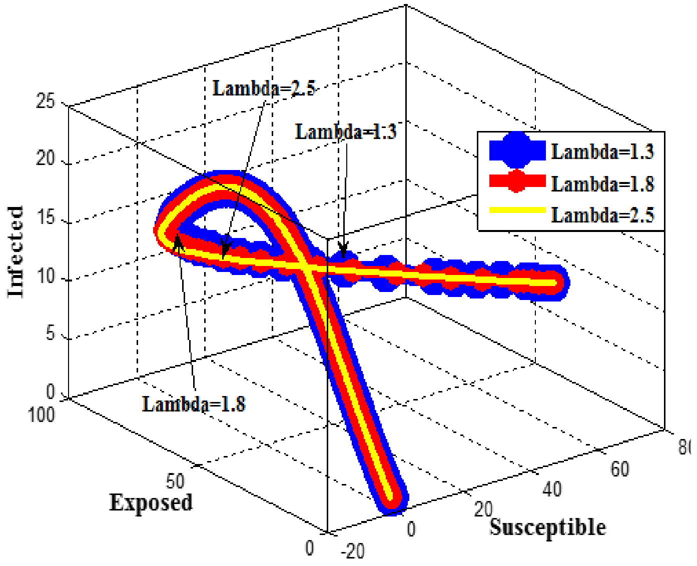

Fig. 20. 3D plot of the SEIR-S model without IPV4 for S, E, I compartments

D. The SEIR–V Model

Mishra and Pandey [38] originally proposed the SEIS-V model, however, it was modified to include the expression of IPV4 address space. Therein, they divided the population of computers (*N*) into subgroups of fully Susceptible nodes (*S*), Exposed nodes (*E*), Susceptible nodes with anti-malicious software (*V*), Infectious nodes (*I*). The assumptions for the SEIS-V model include; *b*: birth rate, *δ*: is the uniform natural death rate as result of hardware failure. Additionally, we assumed the IPV4 address space for the scan-based worm which results to an effective contact rate of *βSI/N* at standard incidence. The original model assumed a certain infection incidence (*σβVI/N*) as a result of the inefficacy of the anti-malicious software existing on the vaccinated computers. However, if the worm probes address space of the vaccinated computers due to the inefficaciousness of the installed anti-malicious software, the infection incidence is equivalent to $\sigma\beta VI/\ N*2^{32}$. Other assumptions include; *ρ*: the anti-malicious software rate, *η*: the transition from exposed to the infected compartment, *α*: mortality rate as a result of worm attack, *γ*: the transition from infectious to the susceptible compartment, *ε*: the transition from the vaccinated compartment to the susceptible compartment. The model also represents the possibility of vertical transmission through the increased rate (*θ*) of worm attack introduced at the *I* compartment. The SEIV-S is given as system (5) below:

$$\begin{aligned}\dot{S} &= bN - \frac{\beta SI}{N*2^{32}} - \delta S - \rho S + \gamma I + \varepsilon V\\ \dot{E} &= \frac{\beta SI}{N*2^{32}} - (\delta + \eta)E\\ \dot{I} &= \eta E - (\delta + \alpha + \gamma)I + \frac{\sigma\beta VI}{N*2^{32}} + \theta b\\ \dot{V} &= \rho S - \frac{\sigma\beta VI}{N*2^{32}} - (\varepsilon + \delta)V\end{aligned} \qquad (5)$$

It is noteworthy to mention that we first simulated the model using the standard incidence as was originally proposed by Mishra and Pandey [38]. The resulting behaviour showed that both the presence and absence of IPV4 were not different; the implication is that standard incidence cancels the effect of adding the expression of IPV4 address scanning space. Consequently, we used the mass action incidence for the numerical simulation of the SEIRS model and it resulted in Fig. 21 and Fig. 22. The figures showed some difference. The simulation experiments were done using the following values: β = 0.01, ρ = 0.01, b = 0.01, α = 0.09, η = 0.03, θ = 0.05, ε = 0.02, σ = 0.03, γ = 0.03. The initial values were 100, 30, 20, 50 for *S*, *E*, *I* and *V* respectively. For the vaccinated computers, the responses for the presence (Fig. 21) and absence (Fig. 22) of IPV4 basically originate from 50, but while the former shows the higher tendency to approach equilibrium, the latter shows otherwise. Interestingly, other compartments showed remarkable difference.

In the light of SEIV-S model assumptions, differences were clearly shown using Fig. 23 and Fig. 24, which are the 3D plots of the SEIV-S model. During this simulation, the infectious rates were varied in this manner; β = 0.01, 0.04, 0.08. Specifically, Fig. 23 is the 3D plot of the SEIV-S model with IPV4 representing the dynamics of Susceptible, Exposed and Vaccinated compartments. While Fig. 24 shows the 3D plot of the SEIV-S model without IPV4 for Susceptible, Exposed and Vaccinated compartments.

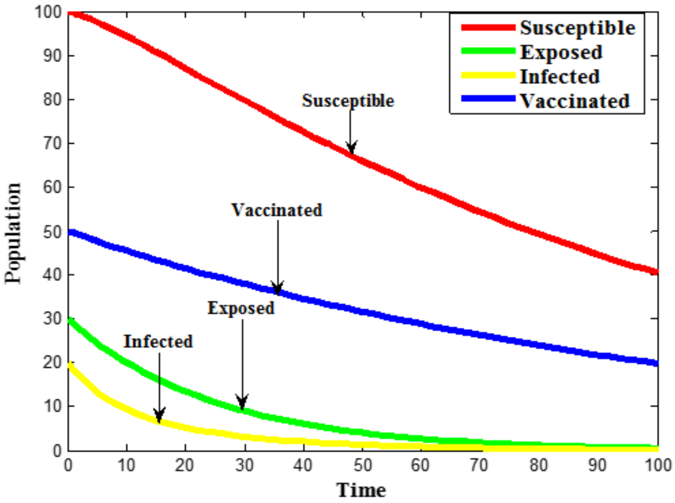

Fig. 21. SEIV-S model with IPV4

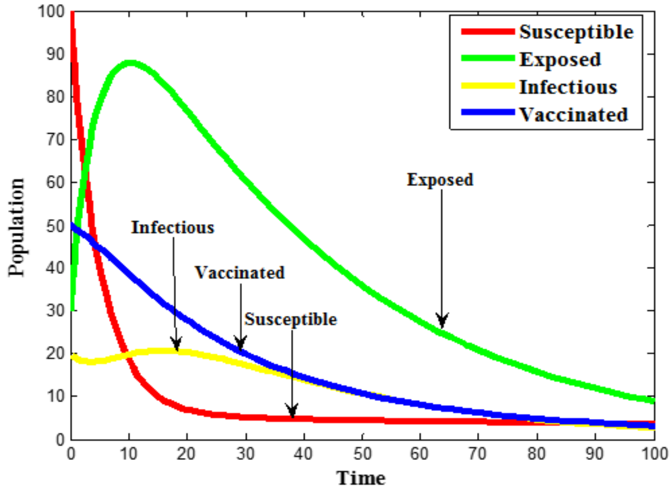

Fig. 22. SEIV-S model without IPv4

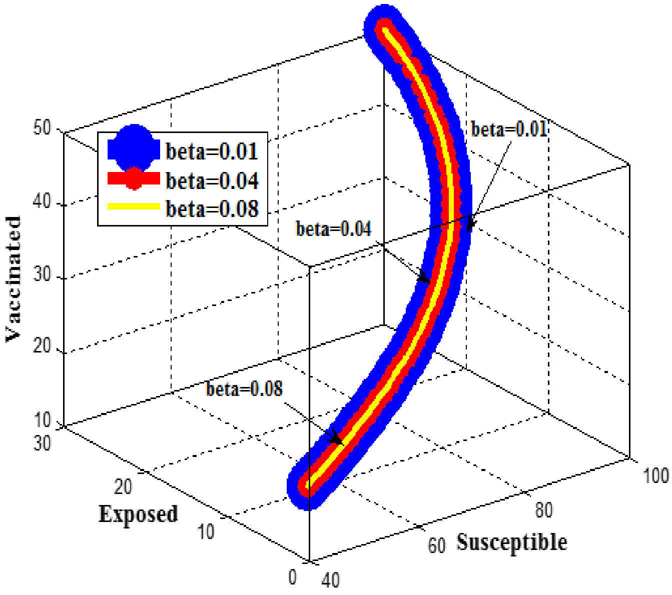

Fig. 23. 3D plot of the SEIV-S model with IPV4 for S, E, V compartments

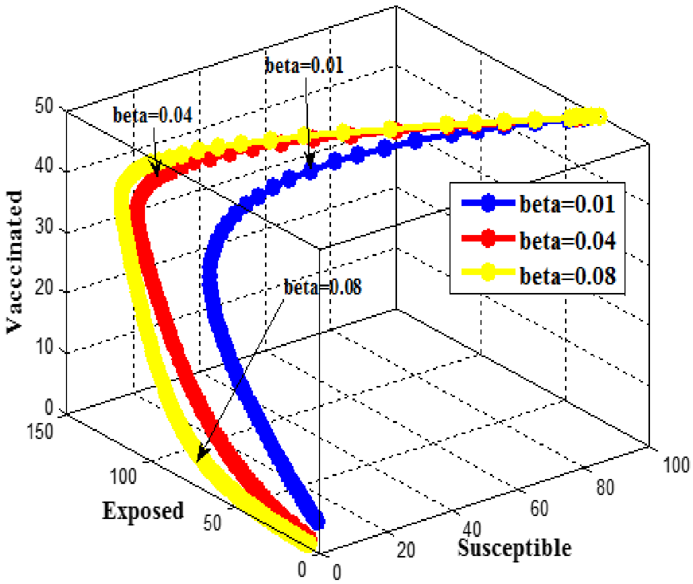

Fig. 24. 3D plot of the SEIV-S model without IPV4 for S, E, V compartments

E. *The SEIR Model*

The e-epidemic SEIR model was originally developed by Mishra and Prajapati [43], therein the population of computers are divided into groups of susceptible, exposed, infected and recovered classes denoted as *S(t)*, *E(t)*, *I(t)*, *R(t)* respectively. The assumptions of the model include; r: the rate of adding new nodes to the computer network, μ: the crashing rate of computers due to worm attack, δ: the crashing of the computers on the network for other reasons, β: infectivity contact rate, k: the carrying capacity, is the recovery of infected nodes and τ: the infection rate in exposed compartment. We added the IPV4 address space resulting to $\beta SI/2^{32}$. The e-epidemic SEIR model is given as system (6) below:

$$\begin{aligned}\dot{S} &= rS - (1 - \tfrac{S}{K}) - \tfrac{\beta SI}{2^{32}} - \delta S\\ \dot{E} &= \tfrac{\beta SI}{2^{32}} - (\tau + \delta)E\\ \dot{I} &= \tau E - (\mu + \delta)I - \rho I\\ \dot{R} &= \rho I - \delta R\end{aligned} \tag{6}$$

Numerical simulations of the SEIRS model using the specified numerical method gave to Fig. 25 and Fig. 26. The simulation experiments were done using the following values: $\beta = 0.05$, $\delta = 002$, $\tau = 0.04$, $r = 0.2$, $k = 100$, $\rho = 0.03$, $\mu = 0.01$. The initial values were 70, 30, 0, 0 for *S*, *E*, *I* and *R* respectively. It is clearly evident that the two results that comprise Fig. 25 and Fig. 26 are very different. The susceptible compartment came down from the initial value (IV) of 70 approaching 0, while for the inclusion of IPV4 it went above the IV. The intersection of the exposed and infectious compartment are different too; while it is at ((20, 50) on (x, y) axes) for the absence of IPV4 (Fig. 25), conversely it was (17, 12 on (x, y) axes) for the presence (Fig. 26) of the address space. The recovered compartments of both results are also clearly different. A close examination using 3D plots of the SEIV-S model displayed internal dynamics with certain differences. These are depicted as Fig. 27 and Fig. 28. During this simulation, the infectious rates were varied in this manner; β = 0.05, 0.09, 0.13. Fig. 27 is the 3D plot of the SEIR model with IPV4 representing the dynamics of Susceptible, Exposed and Infected compartments. While Fig. 28 shows the 3D plot of the SEIR model without IPV4 for Susceptible, Exposed and Infected compartments.

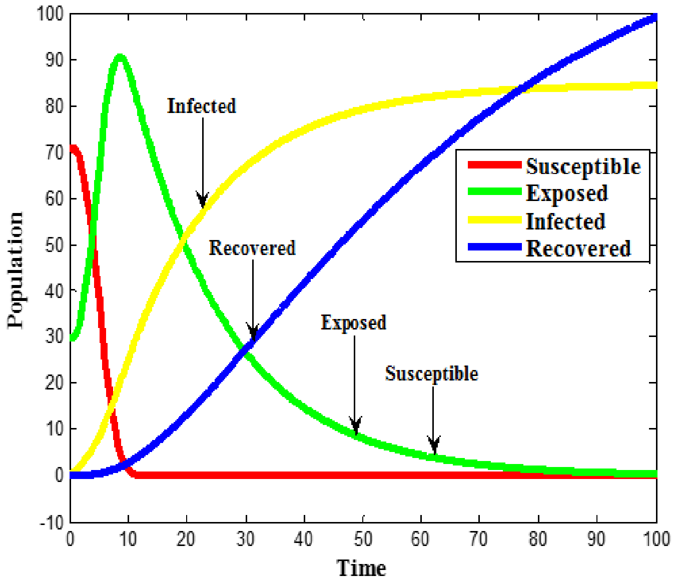

Fig. 25. SEIR model without IPV4

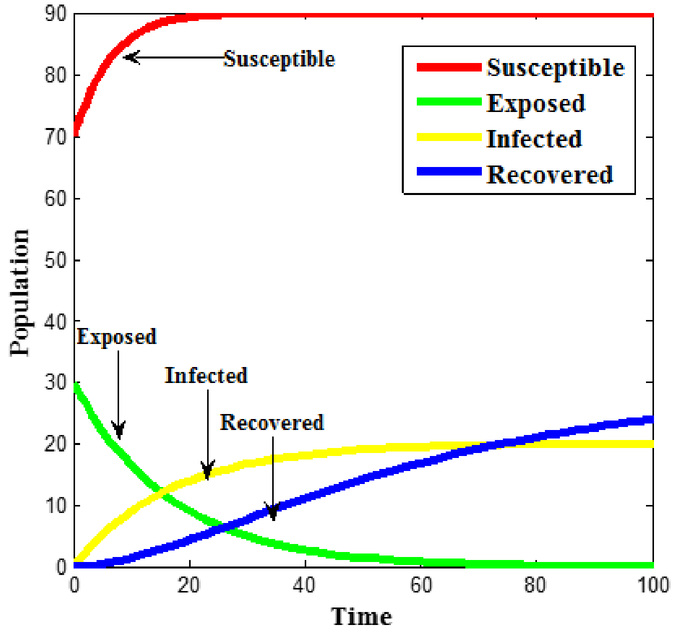

Fig. 26. SEIR model with IPV4

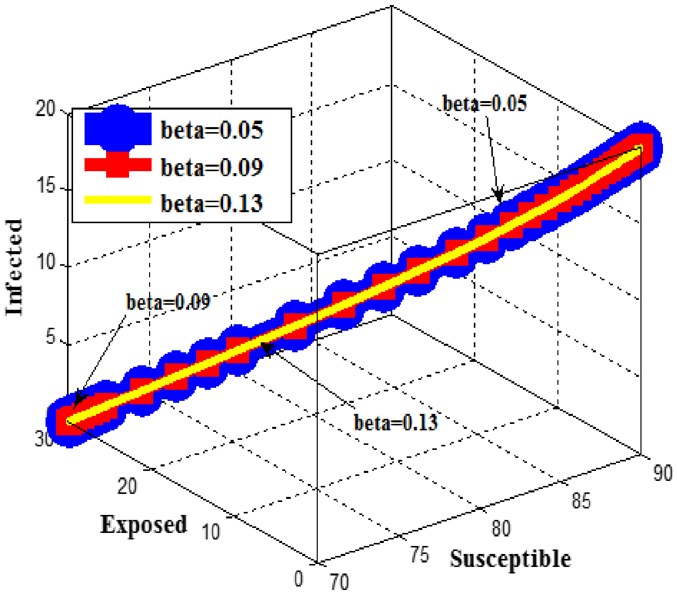

Fig. 27. 3D plot of the SEIR model with IPV4 for S, E I compartments

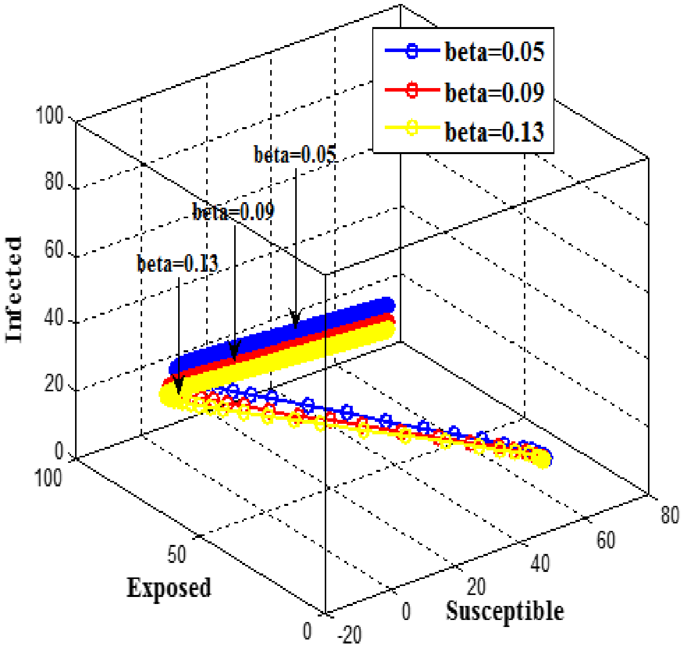

Fig. 28. 3D plot of the SEIR model without IPV4 for S, E, I compartments

F. *The Q-SEIR Model*

The pre-quarantine concept was conceived by Nwokoye, *et al.* [7] for Wireless Sensor Networks. Subsequently, the concept was established as network access control (NAC) and applied in Nwokoye, et al. [9]. Therein, NAC for traditional computer systems can be used to achieve the following; “prevent network breaches, eliminates unauthorized network connections and identify, quarantine and remediate non-compliant/vulnerable devices in the network” [9]. The assumptions of the model include; λ is the inclusion rate of nodes into the network population, β is the infectivity contact rate, d is the mortality or the death rate of nodes due to hardware or software failure, η is the death rate of infected immigrant nodes, δ is the crashing rate due to attack of malicious objects, ϕ is the rate of transmission from Infectious to Recovered class, ε is the rate of transmission from Recovered to Susceptible class, ρ is the rate of transmission from Quarantined to Susceptible class, γ is the rate of transmission from Exposed to Infectious class, ω is the rate of transmission from Quarantine class to Recovered class. With the addition of the IPV4 address space i.e. $\beta SI/2^{32}$, the Q-SEIR model is given as system (7) below:

$$\begin{aligned} \dot{S} &= \rho Q + \varepsilon R - \frac{\beta SI}{2^{32}} - dS \\ \dot{E} &= \frac{\beta SI}{2^{32}} - E(\gamma + d) \qquad (7) \\ \dot{I} &= \gamma E - I(\phi + d + \delta) \\ \dot{R} &= \omega Q + \phi I - R\,(\varepsilon + d) \end{aligned}$$

Numerical simulations of the Q-SEIR model using the specified numerical method gave rise to Fig. 29 and Fig. 30. The simulation experiments were done using the following values: $\lambda = 0.33$, $\rho = 0.3$, $\omega = 0.01$, $\varepsilon = 0.3$, $\beta = 0.1$, $\gamma = 0.25$, $\phi = 0.4$, d = 0.003, and $\delta = 0.07$. The initial values are 100, 3, 1, 0 for *S*, *E*, *I* and *R* respectively. Looking at the susceptible compartments of both results, it is clear that Fig. 29 (presence of IPV4) and Fig. 30 (absence of IPV4) are grossly different. More so, a keen investigation of the 3D plots (Fig. 31 and Fig. 32) of the Q-SEIR model showed similar variations. During this simulation, the infectious rates were varied in this manner; β = 0.1, 0.4, 0.8. Fig. 31 is the 3D plot of the Q-SEIR model with IPV4 representing the dynamics of Susceptible, Exposed and Infected compartments. While Fig. 32 shows the 3D plot of the SEIR model without IPV4 for Susceptible, Exposed and Infected compartments.

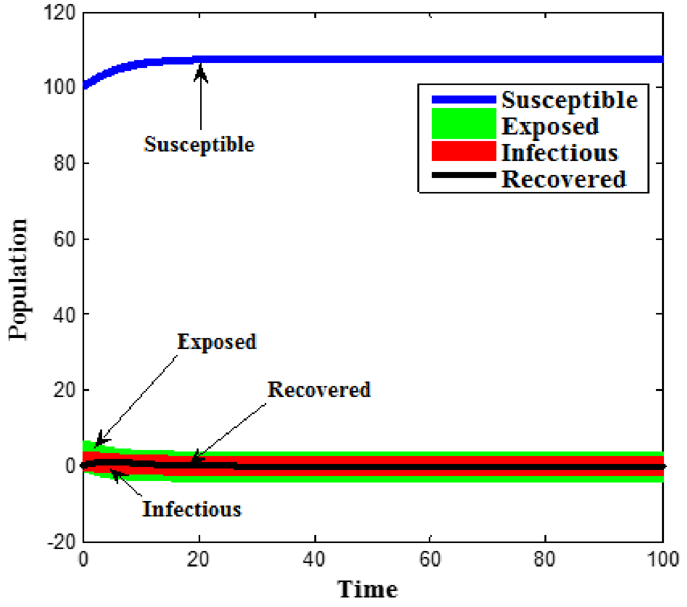

Fig. 29. Q-SEIR model with IPV4

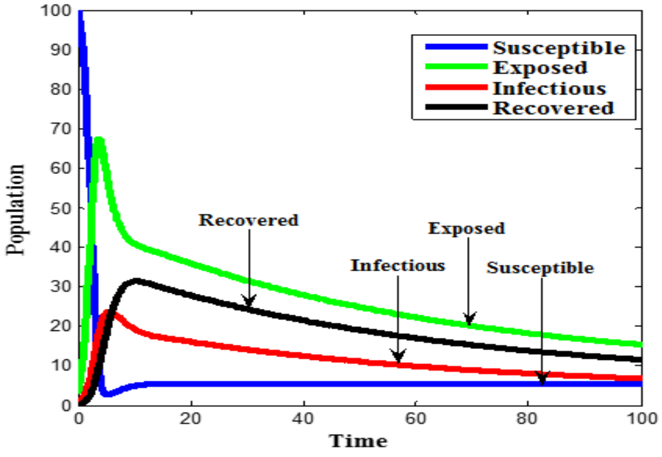

Fig. 30. Q-SEIR model without IPV4

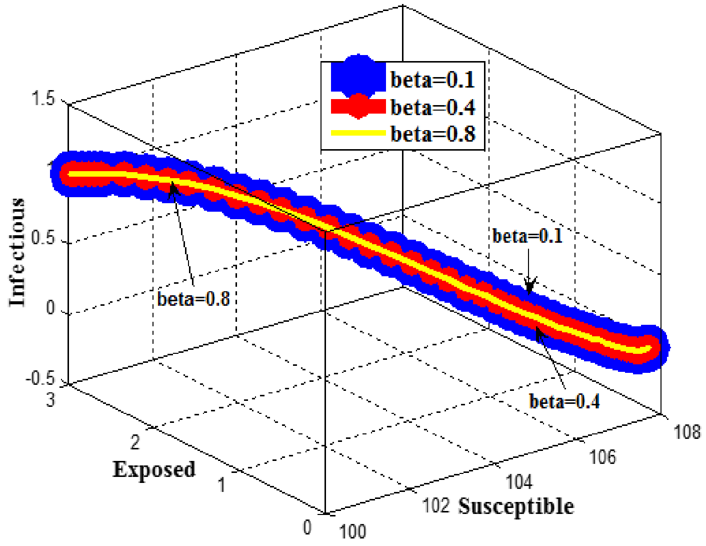

Fig. 31. 3D plot for Q-SEIR model with IPV4 for S, E, I compartments

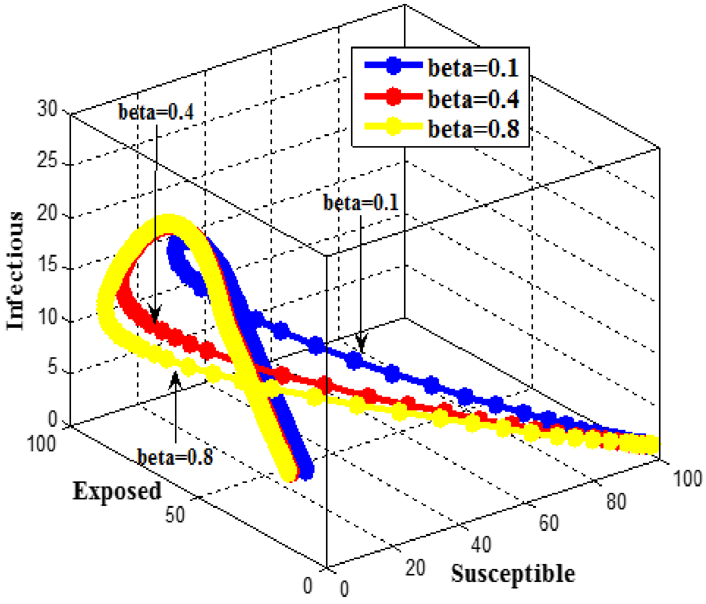

Fig. 32. 3D plot for Q-SEIR model without IPV4 for S, E, I compartments

In the above models, it is noteworthy that the difference between SEIR-S and SEIR is that the former considered re-infection, while the latter does not. For the SEIS–V, instead of recovery, the model considered both vaccination and reinfection. Also, note that in all the 3D simulation experiments, the different rates (β) of san-based worm infectiousness were used. The rationale behind using this parameter is because during homogenous mixing inherent in the above compartmental models, effective transmission basically involves the Susceptible and Infected compartments as well as the infectious rates β. The β parameter for rate of infectiousness was called λ in the SEIR-S model by the original authors, therefore, we retained it in our study herein.

V. Conclusion and Future Directions

In this study, we evaluated the impact of the IPV4 address space on computer network epidemic models using time histories obtained through solving the systems of differential equations with the RK45 numerical method. The analyses was done by x-raying the behaviour of the compartments and the time it take to reach equilibrium. However, for all the models evaluated, the behaviour of the susceptible computers are different in the two cases (presence and absence of IP address space). This difference was also observed for the exposed computers. Other noteworthy differences are as a result of the phenomena addressed in the original models. Firstly, we noted a remarkable difference for the SIRM$_S$M$_I$ model developed by Song, *et al.* [26] and these motivated the study. For models [19, 38, 42 and 43] that involve the exposed compartment, it was observed that it starts off at its initial value then it approaches equilibrium when the IPV4 address was considered. Conversely, when IPV4 was not considered, the exposed compartment first, increases sharply then approaches equilibrium slowly. However, for all the models, the susceptible (S) computer compartments are characteristically different for the presence and absence of IPV4 i.e. it takes quite some time to reach equilibrium. Recall that the S compartment represent the vulnerable nodes of the computer network. This study is necessary because most models that litter the literature did not clearly specify the worm type, hence, presenting misleading results for computer network models. In future studies we would evaluate the impact of these scan type of malicious codes for models of denial of service (DOS), distributed denial of service (DDOS) attacks. Perhaps, the use machine learning [44] or deep learning methods such as Long Short-term Memory Recurrent Neural Networks (LSTM RNN) [45] would be applied for computer network epidemic predictions. More so, the evaluation using numerical simulation experiments would also be extended to capture the impact of address space on multi-group infections models of a computer networks.

References

[1] Y. Wang, S. Wen, Y. Xiang, and W. Zhou, “Modeling the Propagation of Worms in Networks: A Survey,” *IEEE Communications Surveys & Tutorials*, vol. 16, no. 2, pp. 942 – 960, June 2014.

[2] Keigo Taga, Junjun Zheng, Koichi Mouri, Shoichi Saito, and Eiji Takimoto, “Firewall Traversal Method by Inserting PseudoTCP Header into QUIC,” *Proceedings of the International MultiConference of Engineers and Computer Scientists (IMECS)*, Hong Kong, pp. 216-221, 2019.

[3] Hui Miao and Chengjun Kang, “Stability and Hopf Bifurcation Analysis of an HIV Infection Model with Saturation Incidence and Two Time Delays,” *Engineering Letters*, vol. 27, no. 1, pp. 9–17, 2019.

[4] Afeez Abidemi, Mohd Ismail A. Aziz, and R. Ahmad, “The Impact of Vaccination, Individual Protection, Treatment and Vector Controls on Dengue,*” Engineering Letters*, vol. 27, no. 3, pp. 613–622, 2019.

[5] Jian Ding, Tao Zhao, Zhigang Liu, and Qiong Guo, “Stability and Bifurcation Analysis of a Delayed Worm Propagation Model in Mobile Internet,*” IAENG International Journal of Computer Science*, vol. 47, no. 3, pp. 533–539, 2020

[6] C. H. Nwokoye, V. E. Ejiofor, R. Orji, N. N. Mbeledogu and I. Umeh Investigating the Effect of Uniform Random Distribution of Nodes in Wireless Sensor Networks using an epidemic worm model. *Computing Research and Innovation*, 2016.

[7] C. H. Nwokoye, V. E. Ejiofor and C. G. Ozoegwu, “Pre-Quarantine Approach for Defence against Propagation of Malicious Objects in Networks”, *I. J. Computer Network and Information Security*, vol. 9, no. 2, pp. 43 – 52, 2017.

[8] C. H. Nwokoye, N. N. Mbeledogu and I. A. Ejimofor, “The Impact of Sensor Area Types on Worm Propagation using SEIR and SEIR-V Models: A Preliminary Investigation”, *I. J. Wireless and Microwave Technologies*, vol. 7, no. 6, pp. 33–45, 2017.

[9] C. H. Nwokoye, N. N. Mbeledogu, I. Umeh and I. A. Ejimofor, “Modeling the Effect of Network Access Control and Sensor Random Distribution on Worm Propagation”, *I. J. Modern Education and Computer Science*, vol. 9, no. 11, pp. 49-57, 2017.

[10] C. H. Nwokoye, V. E. Ejiofor, M. Onyesolu and B. Ekechukwu, “Towards Modeling Malicious Agents in Decentralized Wireless Sensor Networks: A Case of Vertical Worm Transmissions and Containment”, *I. J. of Computer Networks and Information Security*, vol. 9, no. 9, pp. 12–21, 2017.

[11] C. H. Nwokoye and I. Umeh, “The SEIQR–V model: On a More Accurate Analytical Characterization of Malicious Threat Defense. *I. J. Information Technology and Computer Science*, vol. 9, no. 12, pp.28-37, 2017.

[12] C. H. Nwokoye and I. Umeh, “Analytic-Agent Cyber Dynamical Systems Analysis and Design Methodology for Modeling Temporal/Spatial Factors of Malware Propagation in Wireless Sensor Networks,” *Elsevier MethodsX*, no. 5, pp. 1373–1398, 2018.

[13] C. H. Nwokoye, I. Umeh. and O. Ositanwosu, “Characterization of Heterogeneous Malware Contagions in Wireless Sensor Networks: A Case of Uniform Random Distribution”, *Lecture Notes in Networks and Systems*: *ICT Analysis and Applications*, vol. 2, 2021.

[14] E. Gelenbe, “Dealing with software viruses: A Biological Paradigm”, *Inform. Sec. Tech*. Rep, vol. 12, no. 4, pp. 242–250, 2007.

[15] E. Gelenbe, “Keeping Viruses under Control”, *20th International Symposium Computer and Information Sciences – ISCIS 2005*, Vol. 3733, pp. 304–311, 2005.

[16] C. C. Zou, W. Gong and D. Towsley, “Malicious Codes Propagation Modeling and Analysis under Dynamic Quarantine Defense”, *Proceeding of the ACM CCS Workshop on Rapid Malcode*, pp. 51–60, 2003.

[17] D. Moore, C. Shannon, G. M. Voelker and S. Savage, “Internet quarantine: requirements for containing self-propagating code”, *Proceeding of IEEE INFOCOM2003*, pp. 85–91, 2003.

[18] B. K. Mishra and D. K. Saini, “Mathematical Models on Computer Viruses,” *Appl. Math. Comput.*, vol. 187, no. 2, pp. 929–936, 2007.

[19] B. K. Mishra and S.K. Pandey, “Dynamic Model of Worms with Vertical Transmission in Computer Network,” *Applied Mathematics and Computation*, vol. 217, no. 21, pp. 8438–8446, 2011.

[20] B. K. Mishra and D. K. Saini, “SEIRS Epidemic Model with Delay for Transmission of Malicious Objects in Computer Network,” *Appl. Math. Comput.*, vol. 188, no. 2, pp. 1476–1482, 2007.

[21] B. K. Mishra and S.K. Pandey, “Fuzzy Epidemic Model for the Transmission of Worms in Computer Network,” *Nonlinear Anal.: Real world Appl.*, no. 11 pp. 4335–4341, 2010.

[22] B. K. Mishra and N. Jha, “Fixed Period of Temporary Immunity after Run of Anti-Malicious Software on Computer Nodes,” *Applied Mathematics. Comput.*, vol. 190, no. 2, pp. 1207–1212, 2007.

[23] B. K. Mishra and S.K. Pandey, “Effect of Antivirus Software on Infectious Nodes in Computer Network: A Mathematical Model,” *Phys. Lett. A*, No. 376 pp. 2389– 2393, 2012.

[24] S. Datta and H. Wang, “The Effectiveness of Vaccinations on the Spread of Email-Borne Computer Virus,” *IEEE CCECE/CCGEL*, pp. 219–223, 2005

[25] M. E. Alexander, S. M. Moghadas, P. Rohani and A.R. Summers, “Modeling the Effect of a Booster Vaccination on Disease Epidemiology,” *J. Math. Biol*, no. 52, pp. 290–306, 2006.

[26] L. Song, Z. Jin, G. Sun, J. Zhang and X. Han, “Influence of Removable Devices on Computer Worms: Dynamic Analysis and Control Strategies,” *Computers and Mathematics with Applications*, vol. 61, pp. 1823–1829, 2011.

[27] A. N. Ali, “Comparison study between IPV4 & IPV6,” *International Journal of Computer Science Issues*, vol. 9, no 1, pp. 314 – 317, 2012.

[28] J. R. Piqueira, B. F. Navarro and L. H. Monteiro, “Epidemiological Models Applied to Virus in Computer Network,” *Journal of Computer Science*, vol. 1, no. 1, pp. 31–34, 2005.

[29] B. K. Mishra and D. K. Saini, “SEIRS Epidemic Model with Delay for Transmission of Malicious Objects in Computer Network,” *Applied Mathematics and Computation*, vol. 188, No. 2, pp. 1476–1482. 2007.

[30] B. K. Mishra and D. K. Saini, “Mathematical Models on Computer Viruses,” *Applied Mathematics and Computation*, vol. 187, no. 2, pp. 926-936, 2007.

[31] B. K. Mishra and N. Jha, “Fixed Period of Temporary Immunity after Run of Anti-Malicious Software on Computer Nodes,” *Applied Mathematics and Computation*, vol. 190, no. 2, pp. 1207-1212, 2007.

[32] H. Yuan and G. Chen, “Network Virus Epidemic Model with Point-To-Group Information Propagation,” *Applied Mathematics and Computation*, vol. 206, no. 3, pp. 357 – 367, 2008.

[33] J. R. Piqueira and F. B. Cesar, “Dynamic Models for Computer Virus Propagation,” *Mathematics Prob. Engineering*, vol. 940, no. 526, pp. 1 – 11, 2008.

[34] Piqueira, J. C. and V. O. Araujo, “A Modified Epidemiological Model for Computer Viruses,” *Applied Mathematics and Computation*, vol. 213, no. 2, pp. 355–360, 2009.

[35] B. K. Mishra and P. K. Nayak, “Epidemic Model for Active Infectious Nodes in Computer Sub-Networks,” *International Journal of Signal Control and Engineering Applications*, vol. 2, no. 8, pp. 56-60, 2009.

[36] D. K. Saini, “A Mathematical Model for the Effect of Malicious Object on Computer Network Immune System”, *Applied Mathematical Modelling*, vol. 35, no. 8, pp. 3777–3787, 2011.

[37] B. K. Mishra, U. Kumar and G. Sahoo, “Fixed Length of Infective Period for Attacking Worms in Computer Network,” *International Journal of Applied Engineering Research and Development*, vol. 2, no. 2, 19-31, 2012.

[38] B. K. Mishra and S. K. Pandey, “Dynamic Model of Worm Propagation in Computer Network,” Applied Mathematical. Modelling, vol. 38, no. 7-8, pp. 2173-2179, 2013.

[39] M. Kumara, B. K. Mishra and N. Anwar, “E-epidemic Model on Highly Infectious Nodes in the Computer Network,” *International Journal of Computer Science & Engineering Technology*, vol. 4, no. 9, pp. 1216-1223, 2013.

[40] R. Vigneswaran and S. Kajanthan, “Analysis of the Convergence of More General Linear Iteration Scheme on the Implementation of Implicit Runge-Kutta Methods to Stiff Differential Equations,” *IAENG International Journal of Applied Mathematics*, vol. 50, no. 3, pp. 468–473, 2020.

[41] Jianke Zhang, Xucong Tian, Chang Zhou, and Xiaobao Yang, “A Numerical Method for the Fractional Variational Problems Based on Chebyshev Cardinal Functions,” *Engineering Letters*, vol. 28, no. 3, pp. 751 –755, 2020.

[42] B. K. Mishra and N. Jha, “SEIQRS Model for the Transmission of Malicious Objects in Computer Network,” *Applied Mathematical Modelling*, vol. 34, no. 1, pp. 710–715, 2010.

[43] B. K. Mishra and A. Prajapati, “Cyber Warfare: Worms’ Transmission Model,” *International Journal of Advanced Science and Technology*, no. 63, pp. 83-94, 2014.

[44] Li Wuke, Yin Guangluan, and Chen Xiaoxiao, “Application of Deep Extreme Learning Machine in Network Intrusion Detection Systems,” *IAENG International Journal of Computer Science*, vol. 47, no. 2, pp. 136–143, 2020.

[45] Xu Jiawei, and Tomohiro Murata, “Stock Market Trend Prediction with Sentiment Analysis based on LSTM Neural Networks,” *Proceedings of the International MultiConference of Engineers and Computer Scientists*, Hong Kong, pp. 475–479, 2019.