# The Effect of Internet Protocol Addressing Requirement For Scan-based Worms in Multigroup Computer Network Models

**ChukwuNonso Henry Nwokoye** *chinonsonwokoye@gmail.com*
*Open Studies Unit*
*Nigeria Correctional Service*
*Awka, Nigeria*

**Kenneth Obiakor** *kenchiboy63@gmail.com*
*Department of Pharmaceutical and Medicinal Chemistry*
*Nnamdi Azikiwe University*
*Awka, Nigeria*

**Ikechukwu Umeh** *ikumeh1@gmail.com*
*Department of Computer Science*
*Nnamdi Azikiwe University*
*Awka, Nigeria*

**Abstract**

In recent times, epidemic differential equation models have been used to understand the patterns of malicious objects' propagation in networks. This is necessary since malware attacks on information and communication technology infrastructure have become numerous and threatening to cyberspace. Our study herein posits that older multigroup epidemic computer network models are somewhat not to clear on the type of worm propagated, thereby presenting a generalized conclusions on its behavior. However, it has been observed that the internet protocol (IP) address space has been ignored in several formulations of these models. Therefore, we evaluate the effect of applying the IPV6 address configuration to dthe following models; $SI_1I_2I_3RS$, $S_1S_2S_3IR$, E-$S_1S_2I_1I_2RS$ and $SI_1I_2RS$. This is due to the fact that some worm types (scan-based) either randomly or locally search the address space for vulnerabilities in the network. Using the Runge-Kutta numerical method, we performed numerical simulations in order to highlight existent differences and variations (as time histories and 3 dimensional phase plots) for the presence and absence of the IPV6 address format. The study also showed the impact of the incidence functions used in these epidemic models. Through this study, we were able to present a clear understanding of the dynamics of the computer network, and how IPV6 configuration affect susceptibility and multiple infections (scan-based worms inclusive).

**Keywords:** Computer Network, Worms, IPV6, Epidemic Model, Differential Equations, Cybersecurity.

## 1. INTRODUCTION

Ours is a world of proliferating internet use by individuals (students, enthusiasts, hobbyists) and personnel of businesses and organizations that employ information and communication technology in their daily lives. Indeed, the cyberspace underlined by the internet has become inevitable due to benefits which include universal interconnectedness as well as other range of operations and resources. Buttressing this position, Nwokoye, et al. [1] asserts that, "fundamentally, the internet provides intrinsic support to the ever evolving cyber space, wherein its continual operation offers an avalanche of prospects, ease and benefits". Nowadays, a standalone desktop computer can hold an enormous amount of records that support trade, medi-care, finance, military and other private work [2]. The significance of these information to these industries implies huge losses if ever they are misemployed for crooked aims or altered for

mischievous rationales. Malwares which are often referred to as cyber threats developed by black hat hackers, possesses the ability to disrupt not only email/web services but cause plenty destructions to sensitive transactions for electricity, transportation and healthcare organizations. These cyber threats are in the form or viruses, worms and trojan horses etc., and its distribution is depicted as Figure 1. While computer virus (for instance I LOVE YOU) affix itself to program or file in order to spread in a network, a worm (such as Code Red, Slammer) transfers operational duplicates of itself without any form of human meddling [3]. In the case of a trojan horse, "it secretly performs its operation under the guise of a legitimate program" [2]. Trojans are configured to be additionally irritating when compared to virus/worm because the destruction it causes can be in the form of automatic deletion or defacing of files containing sensitive information. Most times, these malicious codes vigorously exploit the vulnerability of computer applications.

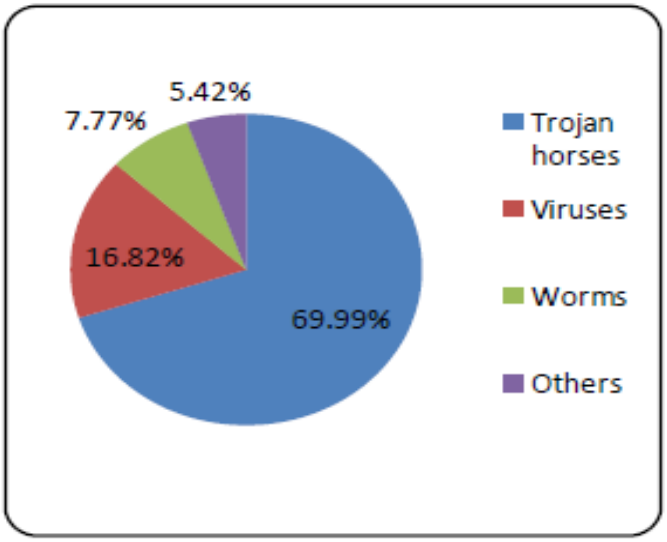


**FIGURE 1:** The Distribution of Cyber Threats [2].

In the light of computer network vulnerabilities, Chebyshev et al. [4] analyzed applications used by cyber criminals during cyberattacks. The identified applications (depicted as Figure 2) include Microsoft Office, browsers, android, java, adobe flash and documents in portable document format (PDF). As Chebyshev puts is, "The increasing popularity of exploits for Microsoft Office suggests that cybercriminals see it as the easiest and fastest way to deploy malware on victim computers" [4]. In order to control and eliminate the devastating tendencies of these malicious codes, researchers have expended enormous efforts and funds into creating anti-malwares that furnish computer systems with some form of transient immunity, which is summarily lost as a result of the emergence of several malware variants.

However, added to the above list of vulnerabilities is the internet protocol (IP) address space exploited by worms [3]. Wang et al. [3] presented several classifications of worms i.e. the scan-based (SBW) and topology-based worms (TBW). For the former, which is our interest in this study, they 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". Scanning strategies include random and localized scanning [3]. The implication is that prior to when the worm pervade the network, it first of all, investigates its weaknesses and enlists diverse target discovery strategies to infect the computer system. Furthermore, this infected node is now used to automatically outspread itself (SBW) or by human triggering (TBW) pervades the network.

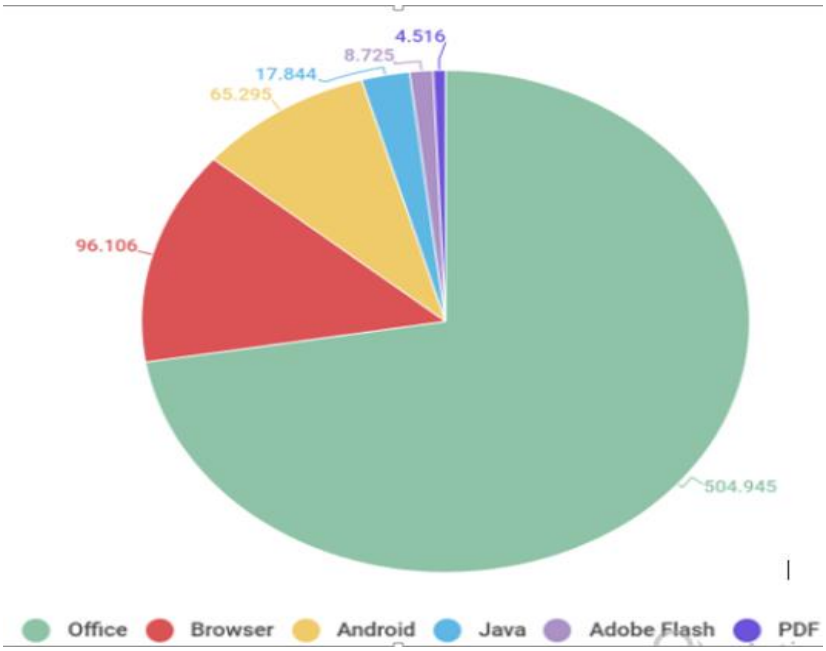


**FIGURE 2:** Distribution of exploits used by cybercriminals, by type of attacked application, Q2 2019 [4].

Combatting cyber threats is of utmost importance since most people depend on the computer and its networks to produce, keep, handle, organize and protect essential data and information transmitted over the internet against loss, destruction and abuse. An anti-malware is used to search out malicious codes by evaluating their definitions and signatures, this is called the black listing strategy. In addition, a fundamental approach for understanding malware spread patterns is by using compartmental models wherein the host population is divided into several groups based on their health status. This concept originated from public health and this is due to the similarities between malwares and the biological disease causing agents. This compartmental models are usually in form of systems of differential equations. Mathematical models help provide deeper understanding into complex malicious objects' propagation schemes and containment approaches. In communication networks (computer and wireless [5-11], compartment models have been used to characterize one type of malware as well as the multiple malicious objects.

Since these worms scan the internet protocol address space, it is needful that studies explore its implications for malicious code spread. Aside the work done by Song, et al [12], most epidemic computer network models have been absent this essential phenomena. Note that the network layer of the Transmission Control Protocol/Internet Protocol (TCP/IP) contains the two well liked kinds of address spaces, namely the IP version 4 (IPV4) and IP version 6 (IPV6). To a large extent, the network layer is the solution to the challenge of internetworking i.e. it directs and oversees the task of packet transfer from a source to an endpoint. IPV4 is basically the 32-bit addressing arrangement with $2^{32}$ addresses (or 4.294.967.296 addresses); while the IPV6 is the 128-bit addressing configuration which contains $2^{128}$ addresses (or 3.4*1038 addresses). These two formats vary in terms of addressing and routing, security, network address translation, administrative workload, and support for mobile devices [13]. At another venue, we have evaluated the impact of IP addressing using differential equation models, but here, we would assess its implication for multigroup models of malicious code infections in computer networks. Specifically, we used the IPV6 due to the successful application of IPV4 in a computer network model by Song et al. [12].

## 2. RELATED WORKS

Epidemic models in computer networks are reviewed here; these models represent the transmission of one type of malware as well as more than one type of malicious objects. By

keenly looking at these models, one can evidently see that they did not represent either of the IP addressing formats while modeling malicious code propagation.

On the one hand, the following are models that represent the spread of one type of infection in a network. Piqueira, et al. [14] altered the original Kermack and Mckendrick's Susceptible-Infected-Removed (SIR) model by adding a compartment, which they called "anti-viral" for the treatment of infected nodes, thus forming the SIRA model. Mishra and Saini [15] developed a model for epidemic transmission in computer networks, consisting of integro-differential equations and they called it the Susceptible-Exposed-Infected-Recovered-Susceptible (SEIRS) model. Its assumptions include a mortality rate of ((I - p)) due to malware attack, a constant mortality rate for hardware or software failure, and a transient immunity by a probability of P (O≤P≤I). Mishra and Saini [16] formulated four epidemic models for computer virus spread, wherein infection is possible at various conditions. The Susceptible-Infected-Recovered (SIR) epidemic model was formulated by Mishra and Jha [17]. This model possesses a constant period of transient immunity as a result of an ephemeral recovery from malicious code infection. Yuan and Chen [18] suggested the Susceptible-Exposed-Infected-Recovered (SEIRS) model to cater for network virus spread. Taking a different directions from existing models, the models addressed three essential network issues namely; different states of the anti-malware, latency periods prior to full infectiousness of a node and the point-to-group information spread pattern. In order to generate a model that is well adapted to computer networks, Piqueira and Ceasar [19] built the Susceptible, Antidotal, Infectious, and Contaminated (SAIC) model through simple systems identification approach; and validated it using real data of computer viruses. Piqueira and Araujo [20] presented an upgrade to the existent SAIC model by representing the dynamics inherent in including a network of computer systems wherein anti-virus programs are installed. Mishra and Nayak [21] modified the Susceptible–Infectious (SI) model in order to address sub-networks where the infectious class (include both active and non-active nodes) there is continuous interaction between them. Saini [22] posited a radically different approach to malicious code representation through a non-linear analytical model that investigates the behavior of several compartments therein. Unlike the above models that only x-ray horizontal transmission, Mishra and Pandey [23] used the SEIRS model to study the import of worm infection through vertical transmission (VT). A Susceptible-Infectious-Susceptible (SIS) model with reinfection and constant infectious periods as a result of worm attack was proposed by Mishra and Kumar [24]. Three other models resulted from this original SIS model wherein analyses involved VT and time delays. Also, Mishra and Pandey [25] performed a critical analysis of VT and an anti-malicious program using the Susceptible–Exposed–Infectious–Susceptible with Vaccination (SEIS–V) epidemic model. This resulted in a modified epidemic threshold. Kumara, et al. [26] formulated the e-Epidemic Susceptible-Infectious-Highly Infectious-Recovered (SIJR) model to cater for varying infectivity and natural mortality due to hardware or software failure.

On the other hand, we present models for computer networks wherein more than one kind of malicious code can exist in a network at the same time. Note that, "this concept of representing multiple infection types is referred to as multi-group modelling, and was originally investigated in the field of Mathematical Biosciences, where a particular heterogeneous population is divided into several homogenous classes based on behavior" [27]. Our study is aimed at investigating the effect of IPV6 in these type of models. Mishra and Singh [28] proposed a model where the population is divided into several groups; Susceptible (S), $I_1$ (infected by worm), $I_2$ (infected by virus), $I_2$ (infected by Trojan horse) and R (recovered nodes) after the application of anti-malicious software. Mishra and Ansari [29] proposed an electronic differential Susceptible-Infectious-Removed- Susceptible (e-SIRS) for viral and worm propagation in a computer network. Mishra and Prajapati [2] proposed the Susceptible class-1 for virus ($S_1$) - Susceptible class-2 for worms ($S_2$) -Susceptible class-3 for Trojan horse ($S_3$) – Infectious (I) – Recovered (R)) for malicious code transfer in a computer networks. Mishra [30] formulated the Susceptible, Infectious due to worm, Infectious due to virus, Recovered and Susceptible ($SI_1I_2RS$) epidemic model to restrict the impact of malicious codes transmission. In all these models, the reproduction ratio or epidemic threshold was derived. More so, numerical methods were used to solve the systems of equation and simulation experiments were used to show the behavior of compartments. Song, et al. [12]

proposed the Susceptible-Infected-Immunized-Susceptible media-Infected media ($SIRM_SM_I$) model to cater for web scanning and removable external devices. The model employed the IPV4 format in the model as $2^{32}$ and this constitutes the size of the scanning space as well as the probability of locating a vulnerable computer in scan ($S/2^{32}$). Finally, it is noteworthy to state here that the above models inherently assume that mixing and interaction is approximately homogenous and therefore, involves incidence rates (i.e. force of infection). Describing two popular types of incidence, Safi et al. [31] posits thus; "If β(N) = βN (i.e., the contact rate depends on the total population, N), then the incidence function g1(I) = βI is called mass action incidence and if β(N) = β (a constant), then the incidence function g2(I) = βI/N is called standard incidence".

## 3. METHODOLOGY

We would modify the above multigroup infection models by adding the expression for IPV6 addressing format. Alongside, other malware types in each model, the resulting models now characterize the scan-based worms that scan IP addresses for vulnerabilities. Subsequently, since the models (system of differential equations) are posed like an initial value problem, the Runge-Kutta order 4 and 5 (RK45) method would be used to solve them. Finally, time histories and three dimensional (3D) phase plots, which are results of simulations experiments, would be used to present the effects of IPV6 scan space in epidemic computer networks models. The parametric values of the original models were adapted for the numerical simulation. Note that throughout the paper, the simulation results on the left hand side (LHS) and right hand side (RHS) depicts the absence and presence of IPV6, respectively.

### 3.1 The $SI_1I_2I_3RS$ Model with Different Infectivity and Mass Action Incidence

The $SI_1I_2I_3RS$ model by Mishra and Singh [28] has several parameters and they include; $q_j$ which is the probability of infective nodes entering into the subgroups of Ij from the Susceptible compartment, A is the addition of vulnerable nodes to the network, μ is the per capita rate of births and deaths as a result of other issues aside malware attack, $\gamma_1$, $\gamma_2$, $\gamma_3$ are the rates of nodes exiting the infectious compartments $I_1$, $I_2$, $I_3$ and to the recovered compartment respectively, $\alpha_1$, $\alpha_2$, $\alpha_3$ are the death rates of nodes as a result of malware attack in the infectious compartments ($I_1$, $I_2$, $I_3$), and δ is the transfer rate for the recovered compartment to the Susceptible compartment.

$$\begin{aligned} dS/dt &= \mu\,(A - S) - q_j\sum\beta_j I_j S + \delta R \\ dI_j/dt &= q_j\sum\beta_j I_j S - (\mu+\alpha_j+\gamma_j)I_j;\ j = 1, 2, 3. \\ dR/dt &= \sum\gamma_j I_j - (\mu+\delta)R \end{aligned} \tag{1}$$

The original assumptions of the original model (system of equations (1)) are retained and further decomposed for the addition of the IPV6 address space and the result is system (2).

$$\begin{aligned} dS/dt &= \mu\,(A - S) - q_1\beta_1 I_1 S/2^{128} - q_2\beta_2 I_2 S - q_2\beta_3 I_3 S + \delta R \\ dI_1/dt &= q_1\beta_1 I_1 S/2^{128} - (\mu + \alpha_1 + \gamma_1)\, I_1 \\ dI_2/dt &= q_2\beta_2 I_2 S - (\mu + \alpha_2 + \gamma_2)\, I_2 \\ dI_3/dt &= q_3\beta_3 I_3 S - (\mu + \alpha_3 + \gamma_3)\, I_3 \\ dR/dt &= \gamma_1 I_1 + \gamma_2 I_2 + \gamma_3 I_3 - (\mu + \delta)R \end{aligned} \tag{2}$$

Numerical simulation was done using the following initial values for the compartments; S=9500, $I_1$, $I_2$, $I_3$=1000, R=0. The values of other parameters of the model include μ=0.05, A=0.009, $\beta_1$=0.005, $\beta_2$=0.005, $\beta_3$=0.005, $\delta$=0.005, $q_1$=0.26, $q_2$=0.27, $q_3$=0.28, $\alpha_1$=0.992, $\alpha_2$=0.889, $\alpha_3$=0.885, $\gamma_1$=0.08, $\gamma_2$=0.07, $\gamma_3$=0.06. The results of numerical simulation include; Figure 3, which is the time histories for $SI_1I_2I_3RS$ model without and with IPV6 while Figure 4 shows the 3D phase plot of the $SI_1I_2I_3RS$ model without and with IPV6 for Susceptible, Infected (Worm) and Infected (Virus) compartments. Looking at Figure 3, one can notice that the two results are different at the

Infected (due to worm) compartment. This difference is clearly shown in Figure 4 where the Infected class is plotted against the Susceptible compartment, while increasing infectious rate.

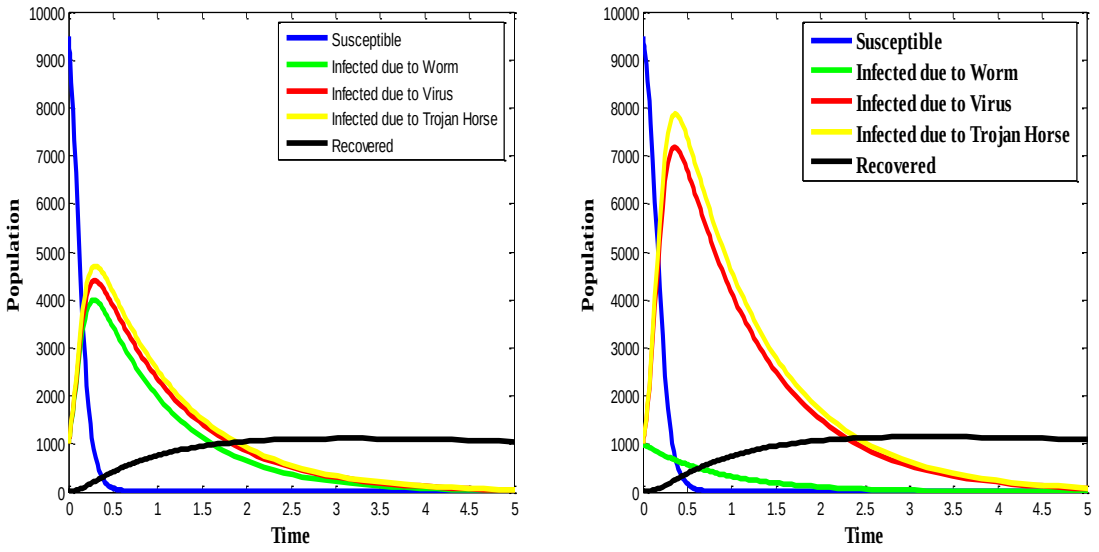


**FIGURE 3:** Time History of The $SI_1I_2I_3RS$ Model without and with IPV6.

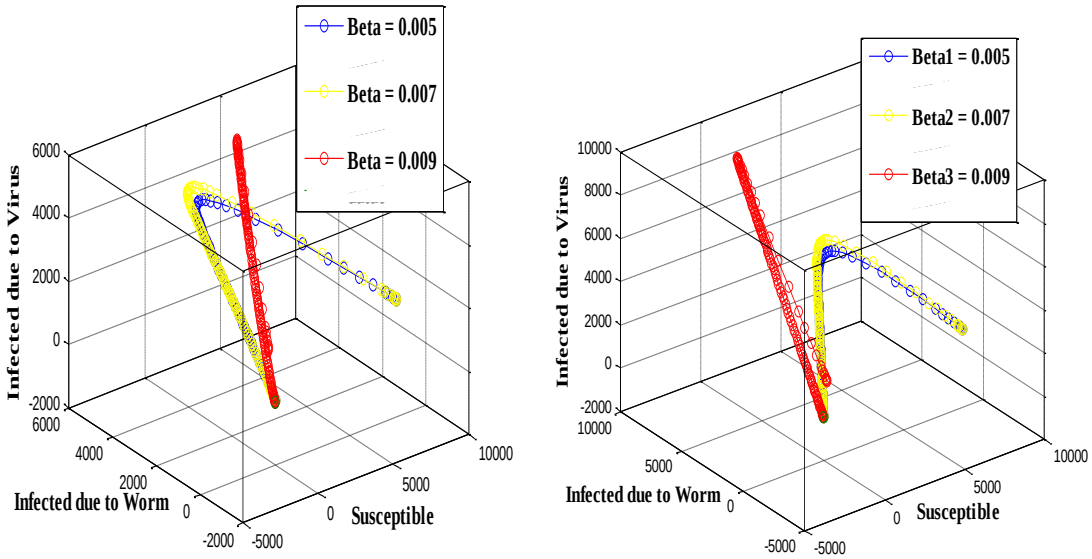


**FIGURE 4:** 3D Phase Plot of the $SI_1I_2I_3RS$ model without and with IPV6 for Susceptible, Infected (Worm) and Infected (Virus) compartments.

### 3.2 The Differential E-SjIjRS Epidemic Model with Standard Incidence

Aside the major compartments i.e. the Susceptible ($S_1$, $S_2$), the infected ($I_1$, $I_2$) and the Recovered (R), the E-$S_jI_jRS$ **(**E-$S_1S_2I_1I_2RS$**)** model by Mishra and Ansari [29] has the following assumptions (or parameters); b=constant birth rate, $m_k$=probability of getting Susceptible by the kth malicious agent, λ=infectivity rate, μ=natural death rate, γ=recovery rate, ε=disease induced mortality rate for recovered nodes, α=vulnerability of Susceptible nodes, β=infectious rate of infected nodes, I/N=probability that a random contact will cause an infection, $p_k$=probability of self-replication of kth malicious agent, $r_k$=self-replication factor of kth malicious agent, $q_k$=probability of recovery from the attack of kth malicious agent, $1–q_k$=probability of non-recovery from the attack of kth

malicious agent, τ=temporary immunity period, ω=latency period, and Φ=time for self-replication of kth malicious agent. Note that λ is equivalent to α.β.c.1/N and k = 1, 2.

$$\begin{aligned} dS_k(t)/dt &= m_k(bN(t)) + (\gamma_k I_k(t-\tau)e^{-\mu\tau}) - \mu S_k(t) - \lambda_k S_k(t) \\ dI_k(t)/dt &= \alpha\beta c I(t-\tau)/N(t-\tau)S(t-\tau).\ e^{-\mu\tau} + [p_k\alpha\beta c I(t-(\tau+\omega+\Phi_k))/N(t-(\tau+\omega+\Phi_k)).S(t- \\ &\quad (\tau+\omega+\Phi_k)\tau_k.e^{-\mu(\omega+\Phi k)})] \\ dR_k(t)/dt &= \sum[q_k\gamma_k I_k(t) - \gamma_k I_k(t-\tau)e^{-\mu\tau} - \varepsilon_k R(t)] - \mu R(t) \end{aligned} \quad (3)$$

The original assumptions of the original model (system of equations (3)) are retained and further decomposed to add the IPV6 address space and the result is system of equations (4).

$$\begin{aligned} dS_1(t)/dt &= m_1(bN(t)) + (\gamma_1 I_1(t-\tau)e^{-\mu\tau}) - \mu S_1(t) - \alpha\beta c I_1(t-\tau)/N(t-\tau).S_1(t-\tau).e^{-\mu\tau} \\ dS_2(t)/dt &= m_2(bN(t)) + (\gamma_2 I_2(t-\tau)e^{-\mu\tau}) - \mu S_2(t) - \alpha\beta c I_2(t-\tau)/N(t-\tau)*2^{128}.S_2(t-\tau).e^{-\mu\tau} \\ dI_1(t)/dt &= \alpha\beta c I_1(t-\tau)/N(t-\tau)S_1(t-\tau).e^{-\mu\tau}+[\ p_1\alpha\beta c I_1(t-(\tau+\omega+\Phi_1))/N(t-(\tau+\ \omega+\ \Phi_1)).S(t- \\ &\quad (\tau+\omega+\Phi_1))\tau_1.e^{-\mu(\omega+\Phi 1)})] \\ dI_2(t)/dt &= \alpha\beta c I_2(t-\tau)/N(t-\tau)S_2(t-\tau).e^{-\mu\tau}+[\ p_2\alpha\beta c I_2(t-(\tau+\omega+\Phi_2))/N(t-(\tau+\ \omega+\ \Phi_2)).S(t- \\ &\quad (\tau+\omega+\Phi_2))\tau_2.e^{-\mu(\omega+\Phi 2)})] \\ dR(t)/dt &= [q_1\gamma_1 I_1(t) + q_2\gamma_2 I_2(t) - \gamma_1 I_1(t-\tau)e^{-\mu\tau} + \gamma_2 I_2(t-\tau)e^{-\mu\tau} - \varepsilon_1 R(t) + \varepsilon_2 R(t)] - \mu R(t) \end{aligned} \quad (4)$$

Numerical simulation was done using the following initial values for the compartment; $S_1$=100, $S_2$=97, $I_1$=94, $I_2$=93, R=0. The values of other parameters of the model include; $\varepsilon_1$, $\varepsilon_2$=0.35, b=0.01, $m_1$, $m_2$=0.3, B=0.45, μ=0.3, $\gamma_1$, $\gamma_2$=0.20, $p_1$, $p_2$=0.3, $\tau_1$, $\tau_2$=0.2, $q_1$, $q_2$=0.58, $\Phi_1$, $\Phi_2$=0.5, ω= 10, r=0.01, α=0.01 and c=0.01.

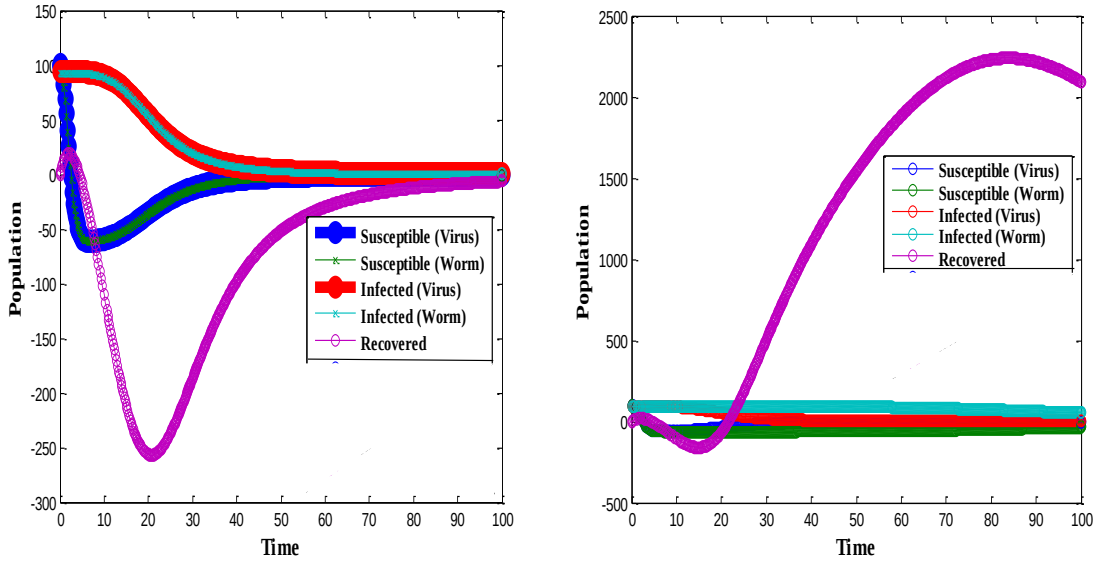


**FIGURE 5:** Time Histories of the E-$S_1S_2I_1I_2$RS Model without and with IPV6.

The results of numerical simulation include; Figure 5, which is the time histories of the E-$S_jI_j$RS model with and without IPV6 for all compartments whereas Figure 6 is the 3D phase plot for the E-$S_jI_j$RS model without and with IPV6 for Susceptible (virus), Susceptible (worm) and Recovered Compartments. Additionally, Figure 7 shows the 3D phase plot for the E-$S_1S_2I_1I_2$RS model without and with IPV6 for Infected (virus), Infected (worm) and Recovered compartments. The E-$S_jI_j$RS model showed some behavioral differences when compared with the $SI_1I_2I_3$RS model above, perhaps, this is due to the sub classes of the Susceptible population. For Figure 5, the difference between the two simulation results are very clear. To a large extent, the result (RHS)

that involved IPV6 is the true behavior of the scan-based worm characterized by the model. These variations are further shown in Figure 6 and Figure 7, where the infectious rate are increased. The radically different result shown for the E-$S_1S_2I_1I_2RS$ model can also be attributed to the standard incidence used herein; other models used the mass action incidence in their formulation.

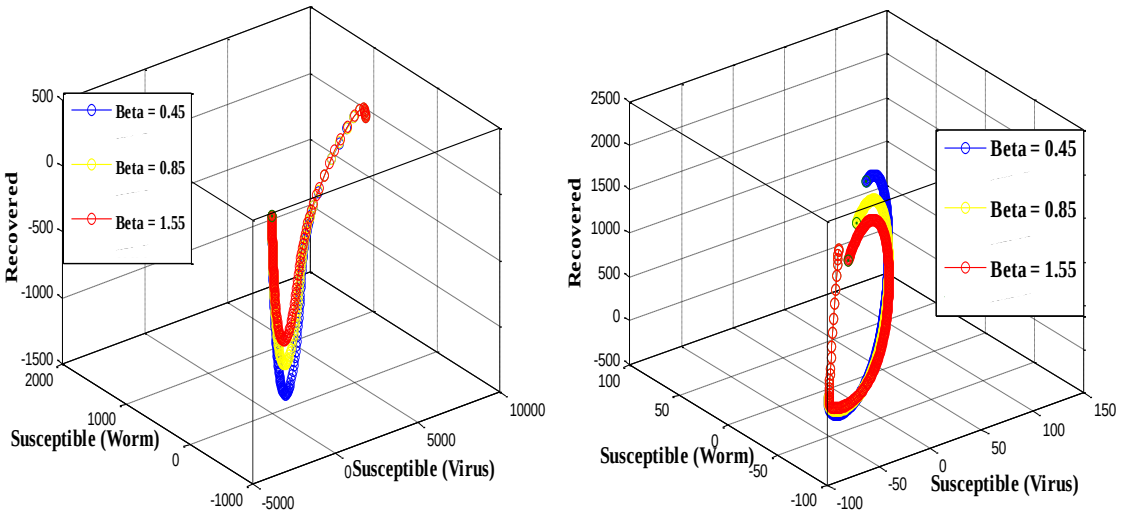


**FIGURE 6:** 3D Phase Plot for the E-$S_1S_2I_1I_2RS$ model without and with IPV6 for Susceptible (virus), Susceptible (worm) and Recovered Compartments.

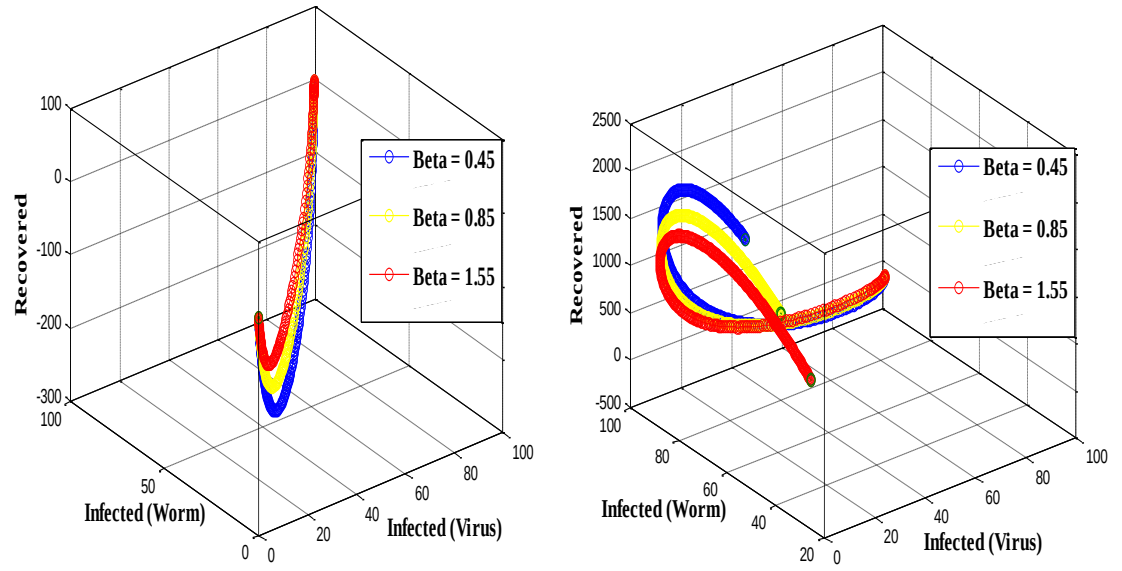


**FIGURE 7:** 3D Phase Plot for the E-$S_1S_2I_1I_2RS$ model without and with IPV6 for Infected (virus), Infected (worm) and Recovered Compartments.

### 3.3 The $S_i$IR Model with Vertical Transmission and Mass Action Incidence

The e-epidemic $S_i$IR (Susceptible class-1, Susceptible class-2, Susceptible class-3, Infectious class and Recovered class) model developed by Mishra and Prajapati [2] shows the changes involved in the transfer of virus, worm and trojans in a computer network. The parameters used in the model are as follows: b is the constant rate at which new nodes are added to the network, d is the death rate of nodes due to natural or non-infectious reason, β denotes the infectivity contact

rate, μ is the recovery rate, δ is the death rate due to attack of malicious codes (virus, worms and trojans), θ is the rate of vertical transmission, $p_i$ is the probability of recruiting nodes from b number of nodes for ith Susceptible class and $\sum p_i=1$ so that the input flow into ith Susceptible class is $bp_i$ (i = 1, 2, 3).

$$\begin{gathered} dS_i/dt = bp_i - \beta S_i I + dS_i \\ dI/dt = \beta I \sum S_i - (d + \mu + \delta - \theta b)I;\ i = 1, 2, 3. \\ dR/dt = \mu I - dR \end{gathered} \tag{5}$$

The original assumptions of the original model (system of equations (5)) are retained and further decomposed to add the IPV6 address space and the result is system (6).

$$\begin{gathered} dS_1/dt = bp_1 - \beta S_1 I + dS_1 \\ dS_2/dt = bp_2 - \beta S_2 I + dS_2 \\ dS_3/dt = bp_3 - \beta S_3 I/2^{128} + dS_3 \\ dI/dt = \beta S_1 I + \beta S_2 I + \beta S_3 I/2^{128} - (d+\mu+\delta-\theta b)I;\ i = 1, 2, 3. \\ dR/dt = \mu I - dR \end{gathered} \tag{6}$$

Numerical simulation was done using the following initial values for the compartment; $S_1$=100, $S_2$=97, $S_3$=94, I=9, R=0. The values of other parameters of the model include; β=0.01, δ=0.05, b=0.01, μ=0.15, d=0.01, θ=0.003, $bp_1$=0.004, $bp_2$=0.003 and $bp_3$=0.003. The results of numerical simulation are as follows; Figure 8 depicts the time histories of the $S_1S_2S_3$IRS model without and with IPV6 while Figure 9 depicts the 3D phase plot for the $S_1S_2S_3$IRS model without and with IPV6 for Susceptible (Virus), Susceptible (Trojan horse) and Susceptible (Worm) compartments. Due to subgroups of the Susceptible compartment, the two results that constitute Figure 8 are somewhat different. This slight difference was also noted when the infectious rates were increased for the 3D plots of Figure 9. The implication is that models with subgroups at the infectious compartment are characteristically different with models where the vulnerable compartment are divided into groups, when mass action incidence is considered. The IPV6 expression impacted heavily the Susceptible due to worm compartment thus elevating its behavior and prolonging the time required to reach equilibrium.

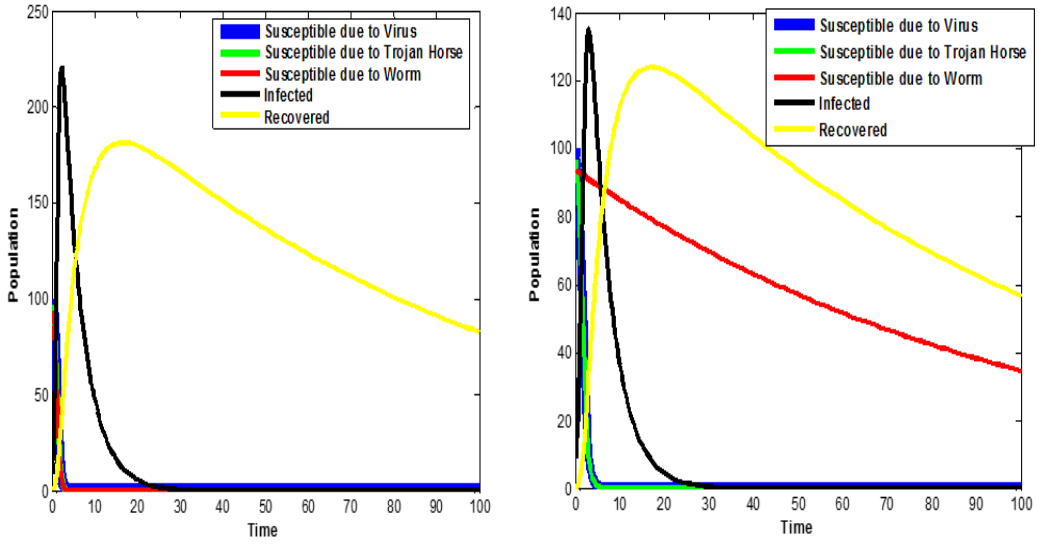


**FIGURE 8:** Time Histories of the $S_1S_2S_3$IRS Model without and with IPV6.

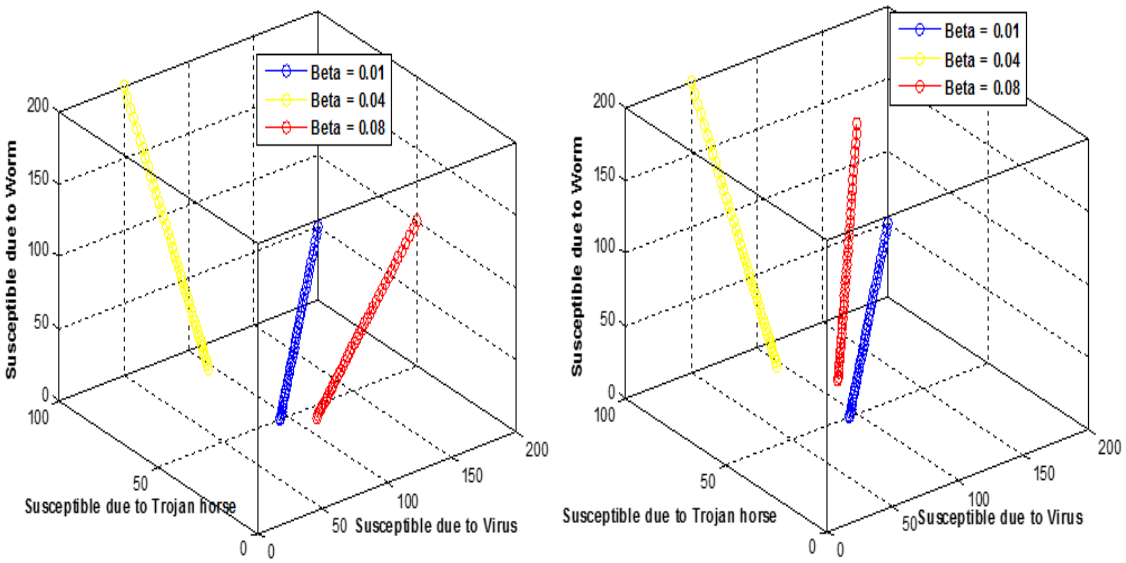


**FIGURE 9:** 3D Phase Plot for the $S_1S_2S_3IRS$ model without and with IPV6 for Susceptible (Virus), Susceptible (Trojan horse) and Susceptible (Worm).

### 3.4 The $SI_1I_2RS$ Model with Different Infectivity and Simple Mass Action Incidence

The $S_I1I_2RS$ Model was originally proposed by Mishra [30] and divided into several groups; Susceptible (S), $I_1$ (Infected by worm) and $I_2$ (Infected by virus) and R (Recovered nodes) after the application of anti-malicious software. For the model parameters, $q_j$ is the probability of infective nodes which enter into the group $I_j$ from the Susceptible class, A is the recruitment of Susceptible nodes in the computer network, μ is the per capita birth rate and death rate due to the reason other than the attack of malicious objects, $\gamma_1$ and $\gamma_2$ are the rates of nodes leaving the Infectious class $I_1$ and $I_2$ to the Recovered class respectively, $\alpha_1$ and $\alpha_2$ are the crashing rate of the nodes due to the attack of malicious objects in Infectious class $I_1$ and $I_2$ respectively and δ is the rate of transmission of nodes from Recovered class to Susceptible class.

$$\begin{aligned} dS/dt &= \mu\,(A - S) - q_j\textstyle\sum\beta_j I_j S + \delta R \\ dI_j/dt &= q_j\textstyle\sum\beta_j I_j S - (\mu + \alpha_j + \gamma_j) I_j + v_j;\ j = 1, 2, 3. \\ dR/dt &= \textstyle\sum\gamma_j I_j - (\mu + \delta) R \end{aligned} \tag{7}$$

The original assumptions of the original model (system of equations (7)) are retained and further decomposed to add the IPV6 address space and the result is system (8).

$$\begin{aligned} dS/dt &= \mu\,(A - S) - q_1\beta_1 I_1 S/2^{128} - q_2\beta_2 I_2 S + \delta R \\ dI_1/dt &= q_1\beta_1 I_1 S/2^{128} - (\mu + \alpha_1 + \gamma_1)\, I_1 + v_1 \\ dI_2/dt &= q_2\beta_2 I_2 S - (\mu + \alpha_2 + \gamma_2)\, I_2 + v_2 \\ dR/dt &= \gamma_1 I_1 + \gamma_2 I_2 - (\mu + \delta) R \end{aligned} \tag{8}$$

Numerical simulation was done using the following initial values for the compartment; S=9500, $I_1$=1000, $I_2$=1000, R=0.The values for the model parameters are as follows; $\mu$=0.05, A=0.009, $B_1$= 0.005, $B_2$=0.005, $\delta$=0.005, $q_1$=0.26, $q_2$=0.27, $\alpha_1$=0.992, $\alpha_2$=0.889, $\gamma_1$=0.08 and $\gamma_2$=0.07. The results of the numerical simulation are; Figure 10, which shows the time histories of the $SI_1I_2I_3RS$ model without and with IPV6 while Figure 11 shows the 3D phase plot of the $SI_1I_2I_3RS$ model without and with IPV6 for Susceptible, Infected (Worm) and Infected (Virus) compartments. The time histories of Figure 10 ($SI_1I_2I_3RS$) are somewhat similar to the Figure 3 (for $SI_1I_2RS$ model), this is because both involved the mass action incidence and possessed subgroups at the infectious compartment. The only difference is that while the former has three subgroups (for viruses, worms and trojans), the latter has two subgroups (for viruses and worms).

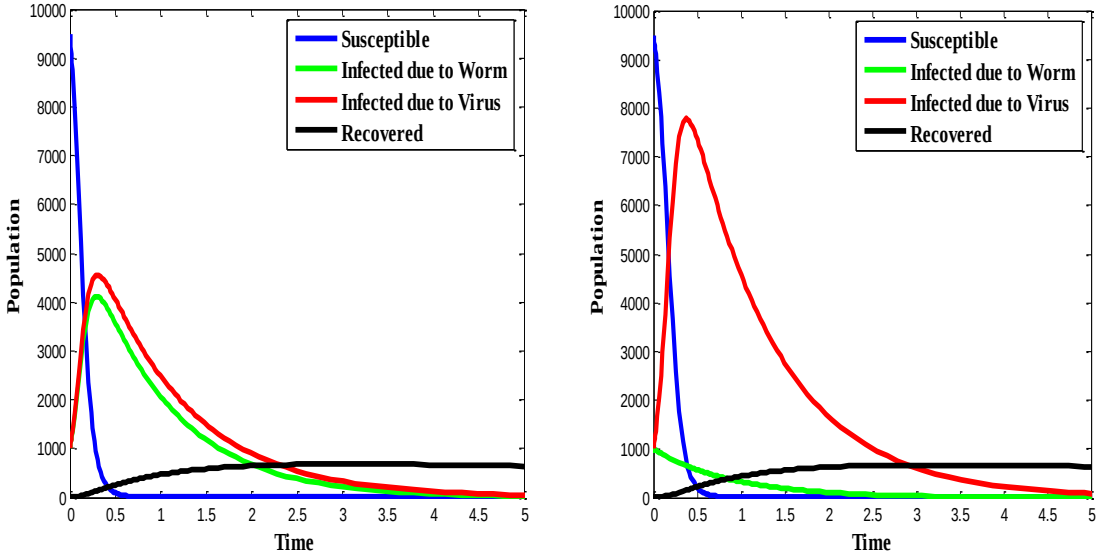


**FIGURE 10:** Time Histories of the $SI_1I_2RS$ Model without and with IPV6.

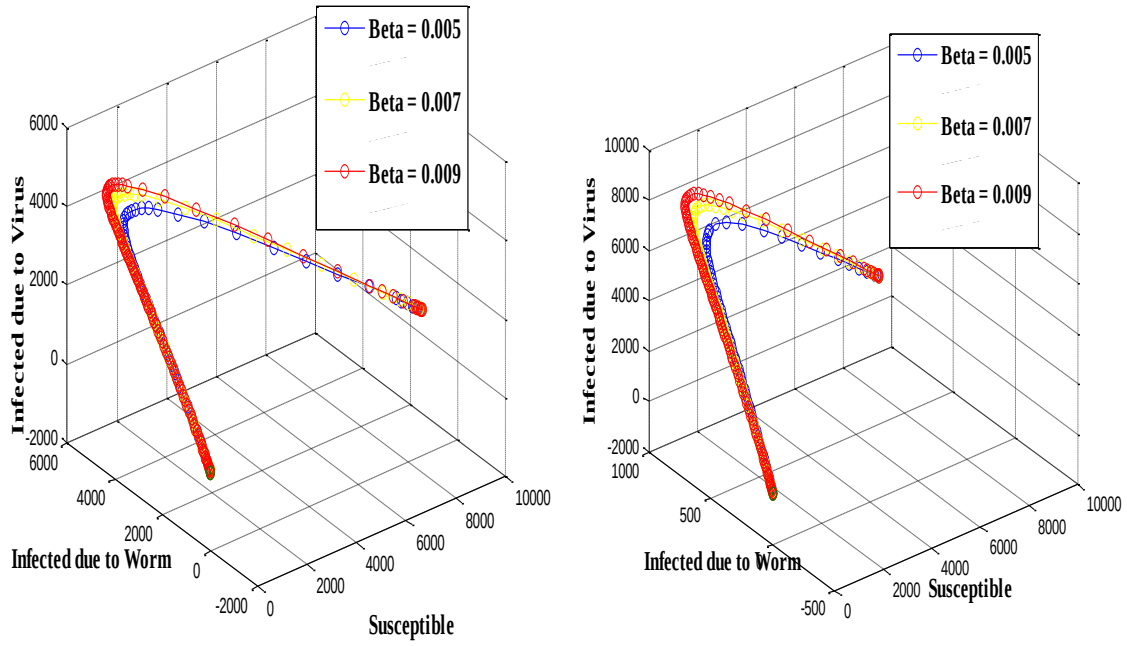


**FIGURE 11:** 3D Phase Plot of the $SI_1I_2RS$ model without and with IPV6 for Susceptible, Infected (Worm) and Infected (Virus) compartments.

### 3.5 Comparative Evaluation using a Model with Similar Configuration

To support and validate the above study, we searched the extant literature on epidemic computer models in order to find other works wherein the IPV6 address format was added in modeling/simulation of spatio-temporal factors of communication networks. We discovered the $SIRM_SM_I$ model proposed by Song et al. [12]. Beside this model and our work herein, there is no other work that evaluates the impact of IP addressing configurations. Song et al. [12] conceived this models so as to cater for internet scanning and detachable external devices. Five classes constitutes this model, and they include Susceptible (S), Infected (I), Immunized (R), Susceptible media ($M_S$) and Infected media ($M_I$). The $SIRM_SM_I$ model is of immense significance to our study

because it represented the IPV4 addressing requirement, wherein $2^{32}$ stands for the size of scanning space and the probability of finding an unprotected computer in a scan, denoted by $S/2^{32}$. For the comparative analyses, the model assumptions were maintained, with the exception of IPV4, which was changed to IPV6. Note that the same numerical method was also used to perform the simulation experiments. During the simulation, the initial values of the compartments are S=310, I=100, R=50, $M_S$=25, $M_S$=15. Other values used include μ1, μ2 ((removal rates of computers and detachable devices) = 0.0027 and δ1 (recovery rates of infected nodes) = 0.033, δ2 (recovery rates of infected media) = 0.0082. The results shown in Figure 12 depicts differences for the presence and absence of the IP address space. Specifically, the Susceptible compartment was raised for the figure on the RHS while, conversely lowered at the LHS. The intersection of Infected and Recovered was lowered at the RHS to 75 from 225 nodes. Figure 13 shows a 3D plot depicting the dynamics inherent through the addition of the IPV6 expression.

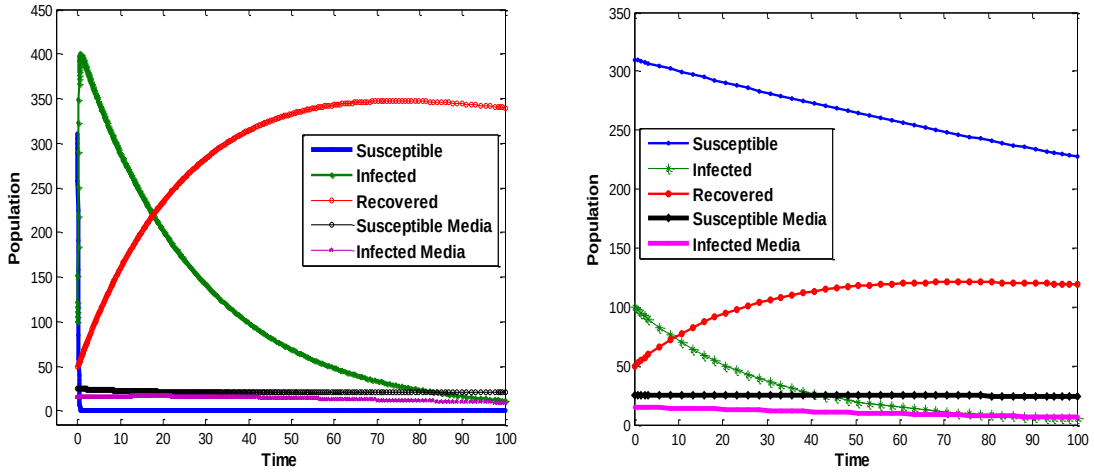


**FIGURE 12:** Time Histories of the SIR$M_S M_I$ Model without and with IPV6.

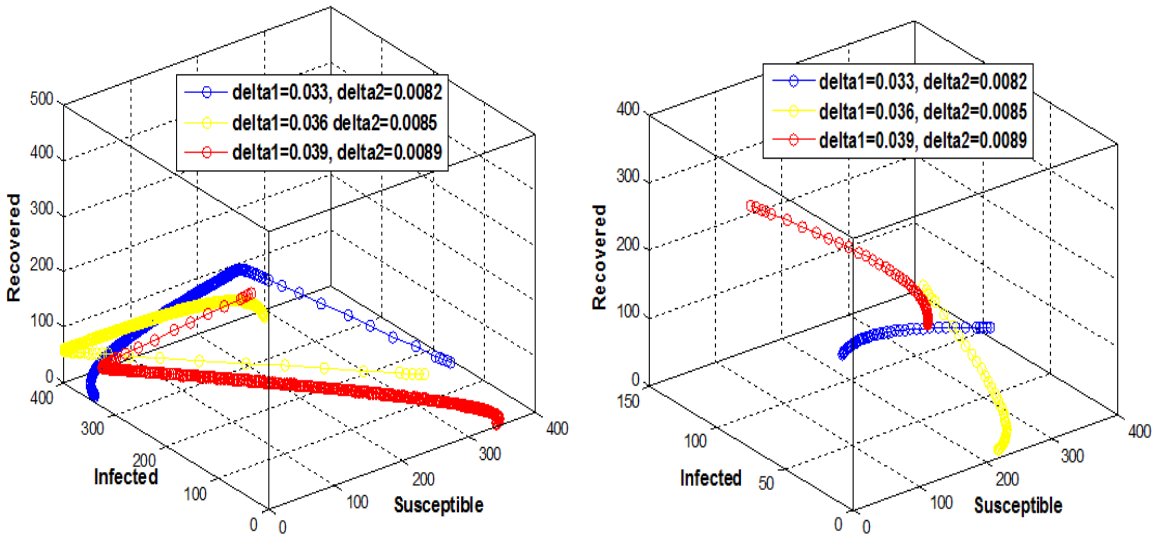


**FIGURE 13:** 3D Phase Plot of the SIR$M_S M_I$ model without and with IPV6 for Susceptible, Infected and Recovered compartments.

## 4. CONCLUSION AND FUTURE DIRECTIONS

In this study, we aimed at evaluating the effects of IP address space on multigroup computer network models gleaned from literature using the RK45 method. Four typical cases wherein the

IPV6 addressing requirement was applied were presented namely; a. Case 1 – the infectious class has three subgroups for worm, virus and trojan; b. Case 2 – the Susceptible and the Infectious class has two subgroups for virus and worm; c. Case 3 – the Susceptible class has three subgroups for virus, worm and trojan; and d. Case 4 – the infectious class has two subgroups for worm and virus. It was discovered that Case 1 and Case 4 showed similar results because they possessed same mass incidence function for homogenous mixing. In addition, the model with standard incidence shows radically different results compared to models with mass action incidence. We also noticed a reduction in the worm Infected class for models $SI_1I_2I_3RS$ and $SI_1I_2RS$; this is the truly infected population after the worm has randomly scanned the population of computers in the network. The validity of our assertions here was shown using the $SIRM_SM_I$ model, which originally has the IP address configuration. Specifically, the absence and presence of IPV6 showed remarkable differences, thus, depicting how scan-based worm distort the general dynamics of epidemic multigroup computer network models. Although, we were able to generate several differences using the RK45 numerical method, in the future, we would investigate the impact of node exposure (or latent) period of worms on IP address space, since none of the above multigroup models included such.

## 5. REFERENCES

[1] C. H. Nwokoye, I. Umeh and O. Ositanwosu. “Characterization of heterogeneous malware contagions in wireless sensor networks: A case of uniform random distribution.” presented at the Proceedings of ICT4SD (ICT Analysis and Applications Vol. 2), India, 2020.

[2] B. K. Mishra and A. Prajapati. “Dynamic Model on the Transmission of Malicious Codes in Network.” I. J. Computer Network and Information Security, vol. 10, pp. 17-23, 2013.

[3] 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, 2014.

[4] V. Chebyshev, F. Sinitsyn, D. Parinov, B. Larin, O. Kupreev and E. Lopatin. “IT threat evolution Q2 2019 Statistics.” 2019. https://securelist.com/it-threat-evolution-q2-2019-statistics/92053/ [Jul. 30, 2020].

[5] 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, Ibadan, Nigeria, 2016.

[6] C. H. Nwokoye, V. E. Ejiofor and C. G. Ozoegwu, “Pre-Quarantine Approach for Defence against Propagation of Malicious Objects in Networks”. International Journal of Computer Network and Information Security, vol. 9, pp. 43 – 52, 2017.

[7] 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”. International Journal of Wireless and Microwave Technologies, vol. 7, pp. 33 – 45. 2017.

[8] 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”. International Journal of Modern Education and Computer Science, Vol. 9, pp. 49-57, 2017.

[9] 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”. International Journal of Computer Networks and Information Security, vol.9, pp. 12–21, 2017.

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

[11] 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”. MethodsX, vol. 5, pp. 1373–1398, 2018.

[12] 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.

[13] A. N. Ali. “Comparison study between IPV4 & IPV6”. International Journal of Computer Science Issues, Vol. 9, pp. 314 – 317, 2012.

[14] J. R. Piqueira, B. F. Navarro and L. H. Monteiro. “Epidemiological Models Applied to Virus in Computer Network”. Journal of Computer Science, Vol. 1, pp. 31–34, 2005.

[15] 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, pp. 1476–1482. 2007.

[16] B. K. Mishra and D. K. Saini. “Mathematical Models on Computer Viruses”. Applied Mathematics and Computation, Vol. 187, pp. 926-936, 2007.

[17] 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, pp. 1207-1212, 2007.

[18] 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.

[19] J. R. Piqueira and F. B. Cesar. “Dynamic Models for Computer Virus Propagation.” Mathematics Prob. Engineering, vol. 940, pp. 1 – 11, 2008.

[20] Piqueira, J. C. and V. O. Araujo. “A Modified Epidemiological Model for Computer Viruses”. Applied Mathematics and Computation, vol. 213, pp. 355–360, 2009.

[21] 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, pp. 56-60, 2009.

[22] D. K. Saini. “A Mathematical Model for the Effect of Malicious Object on Computer Network Immune System”. Applied Mathematical Modelling, vol. 35, pp. 3777–3787, 2011.

[23] B. K. Mishra and S.K. Pandey. “Dynamic Model of Worms with Vertical Transmission in Computer Network.” Applied Mathematics and Computation, vol. 217, pp. 8438–8446, 2011.

[24] 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, pp. 19-31, 2012.

[25] B. K. Mishra and S. K. Pandey. “Dynamic Model of Worm Propagation in Computer Network”. Applied Mathematical. Modelling, vol. 38, pp. 2173-2179, 2013.

[26] 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, pp. 1216-1223, 2013.

[27] C. H. Nwokoye, C. Umeugoji, I. Umeh. “Evaluating degrees of differential infections on sensor networks’ features using the SEjIjR-V epidemic model”. Egyptian Computer Science Journal, vol. 44, pp. 86 – 97, 2020.

[28] B. K. Mishra, A. K. Singh. “SIjRS E-Epidemic Model With Multiple Groups of Infection In Computer Network”. International Journal of Nonlinear Science, vol.13, pp.357-362, 2012.

[29] B. K. Mishra and G. M. Ansari. “Differential Epidemic Model of Virus and Worms in Computer Network”. International Journal of Network Security, vol.14, pp. 149-155, 2012.

[30] B. K. Mishra. “Mathematical Model on Attack of Worm and Virus in Computer Network”. International Journal of Future Generation Communication and Networking, vol. 9, pp. 245-254, 2016.

[31] M. A. Safi and S. M. Garba. “Global Stability Analysis of SEIR Model with Holling Type II Incidence Function.” Journal of Math. Biology, vol. 2012, pp. 1 – 8, 2012.