Enhanced Model for Computer Viruses Counter Measures

[1]D.D. Wisdom, [1]A. Y. Tambuwal, [3]P.B. Chun, [5]H. K. Adamu, [4]E. A. Ajayi
[1]Department of Mathematics, Faculty of Science
Usmanu Danfodiyo University, Sokoto, Nigeria.
danieldaudawisdom1@gmail.com, [2]ahmed-tambuwal@gmail.com

[4]Faculty of Computing and Informatics, Multimedia University, Cyberjaya Campus, Persiaran, Multimedia, Malaysia.
[3]Department of Mathematics,
Plateau State University Bokkos, Jos, Nigeria.
[3]chunpamson@gmail.com,
[4]ebeconsult@myself.com [5]hajrahkhalid@gmail.com

Abstract: *Due to the persistent challenges or risks (viruses) associated with computer devices on the network, a comprehensive study on existing models on computer viruses have been explored to proffer a proper solution to these risks associated with computer systems on the network. Viruses are one of the major challenges on networking environments, for individual PC users, a group of two or more people, organizations and so on. Thus, we propose a new model called, an Enhance Model for Computer Viruses Counter Measures. It employs state transition stages of systematic development and addresses these risks of viruses' re-infection after being immune due to either the anti-virus was stopped because of user drop from alertness, insensitivity or anti-virus uninstalled. We also propose an algorithm of how these viruses propagates as well as derived a mathematical model to show the actual state transition stages of a computer virus and provided a counter measure in order to enhance efficiency, we conducted a simulation and our simulation performance result proved that, the proposed model outperformed the existing ones, in terms of efficiency.*

Keywords: Networking, Computer Viruses**,** Re-infection, Counter Measures, algorithm

1.0 Introduction

Networks and or electronic mail (e-mail), is a growing trend of technological development, which has led to the continues relevance of computer devices globally due to their societal (communication) and economic benefits. The ever-increasing demands and uses of these computer devices such as; mobile phones, Tablets, Desktop/laptop and others have made computing indispensable in our modern days as well as create problems or risks, such as IP spoofing, eaves dropping, Denial of Service attacks, and computer viruses (codes) whose risks are on the raise due to its capability of propagating self. Thus, the increase in the risks of computer viruses, since viruses are series of codes with an ability to propagate through a medium and course harm [6]. Hence, computer virus is still a serious challenge to organizations, individuals and the research community at large [6]. Viruses are programming codes designed to course a computer to behave abnormally or damage the computer system by either altering the original information or completely deleting data files, thus, the need to carry out studies and design model that will reduce/eliminate or counter these challenges faced in this ever-growing networking age.

Studies on computer viruses' countermeasures are divided into two categories, which are mainly, micro and macro studies.

Micro studies are carried out to primarily detect as well as remove individual viruses [13], while studies at the macro Level is carried out in order to analyze the nature of the computer viruses spreading into the network [12]. Several models [11], [9], [3], [7], [13] [12], [10], [6], [10], have been proposed for these studies however, these models have not been able to appropriately provide a lasting countermeasure to these risks associated with computer systems on the networking environment or e-mail. A new approach called Enhance Model for Computer Viruses Counter Measures have been proposed in order to minimize/eliminate the risks that are associated with computer systems via electronic mail. Unlike the existing models [15], [18], which ignored considering re-infection due to the un-installation of an anti-virus software or a slight drop from a user alertness otherwise insensitivity to the settings of the installed software, which may result to a vulnerability of a user PC on the network. Hence, the proposed enhance model for computer viruses counter measures which is a modification of the existing models namely, Dynamic Models for Computer Viruses as well as analysis of a model of computer viruses spreading via e-mail.

Our proposed model addressed these existing risks by designing a suitable model which considers scenarios where computer systems or devices may have been re-infected due to either, that the anti-virus software is stopped because of user insensitivity, otherwise drop from alertness or as a result of un-installation of anti-virus software. The re-infected systems are separated or removed from the network, where these PCs are properly treated and finally immunized with better and reliable anti-virus software. This paper focus mainly on educating individual users on viruses' re-infection as well as a proper treatment and immunization of these individual PCs with a stronger anti-virus in order to minimize higher risks of viruses' re-infection or possibly prevent viruses' propagating to already immune PCs.

1.1 Electronic Viruses

Electronic or E-mail is one of the important medium of information and communication exchange via the network. Viruses capable of replicating themselves through email either via exchanging of messages or file downloads are known as electronic viruses. These E-mail viruses have distinct features such as, propagate: which is the ability of the viruses to replicate from one or more email address stored on a personal computer (PC). Latent: that is when the viruses already propagate self, so it will not propagate further even if it is executed again. More so E-mail viruses do not mutate themselves i.e. viruses do not change from the original programming codes. Finally, viruses are made up of files which may become active when run on a computer system.

1.1.0 Spread of Electronic Viruses

There is a continues data or information exchange on the networking environment from PC to PC. Thus,
Virus propagation takes place from one PC to another due to either exchange of information from one PC to another on the network i.e. connections of PCs on a group of network or as a result of the spatial distribution of PCs on the network especially when there are likely cases of infected PCs inclusive in a group on the network. These transfers take place very fast within a very short period of time; the larger a group of user PCs on a network, the likely the chances of viruses transferred, and the more vulnerable the immediate otherwise adjacent PCs are for infection/re-infection. Therefore, measures have to be taken in order to prevent damage on a computer system(s). Hence, an enhance model for viruses' counter measures has been created which may be used to prevent viruses' attacks on personal computers.

1.1.1 Viruses Spread on the Network

Viruses usually seeks for a medium to propagate, E-mail address stored on personal computers are the easiest means of which viruses propagate to individual computers. The networking range in between a user PC A, and another user PC B is the range between PCs on the network as well as the number of E-mail address registered by a user in an address book, can be said to be the number of connections. More so, the array space is one-dimensional, and each node will represent one PC or user. The closeness of individual social relations is approximately proportional to the number of shared E-mail address [10], [4]. The closer an individual social relation on the network, likewise the number of his/her shared E-mail addresses. PCs address book use to store E-mail addresses are another means of the spread of viruses on the network. In our proposed model, nodes that may be connected to one another are referred to as immediate PCs, and the minimum number of connections on this model is two PCs.

1.1.2 Personal Computers (PCs) State Transitions

Our model divides the states of a user's PC from one form to another as follows:
Susceptible (S) state, infected (i) state, immune (IM) state, Re-infected (Ri) state. The infected state is further divided into two; propagate (P), and latent (L) states.
The states are defined as follow:
Susceptible (S) State: is a state where PCs are void of viruses but a PC may be subsequently infected. Infected PCs may also not be active until when executed by the user. In this situation, a user PC receive the viruses but may not also receive the E-mail with the viruses.
Infected (i) State: is a state where the PCs have been infected already with viruses and are being executed or run. These states include the propagate state, where the viruses propagate to their immediate PCs on the network and the latent state, in which the viruses are waiting for chances to activate and unleash their payloads such as malicious activities (exchange of original information into meaningless form, corrupt files or unexpected disk format). The propagate state is the earlier state of the infection state. Then transition takes place from the propagate state to the latent state there after the viruses. Latent state continues until the viruses are discovered, mostly a PC user, uses an infected PC without knowing that viruses are residing on the background and could course harm or damage on the PC. Such challenges we intend to address.
Immune (IM) State: is a state where PCs are protected either with the help of anti-virus software or the PCs are completely not yet introduced to the network or removed from a particular group on the network.
Re-infection (Ri) State: This occurs when an anti-virus software is uninstalled or an individual PC is stopped due to a user drop from alertness or sensitivity. Thus, in our proposed model, we focus on dealing with viruses' re-infection due to un-installation of the anti-virus software, insensitivity or a drop from a user alertness, in other words after re-infection occurs, individual re-infected PC are discovered and recovered the immune state is the final state. Hence, we have proposed a states transitional model in section 4 Seen bellow.
The rest of this paper is organized as follows: Section 2 discusses on related work. Section 3 explains the key concepts of viruses and its risks and describes the state transition stages of viruses' infection as well as re-infection. Section 4 describes our proposed model. Section 5 concludes this paper.

2.0 Related work

This section presents related research literatures on already existing models. These models are reviewed by highlighting their Operational state transition procedures, strength and weaknesses as follows:

A new analytic numeric method solution for fractional modified epidemiological model for computer viruses was proposed in [1], in order to prevent risks associated to computer security. It considers SAIR model as well as employ a Multi-Step Generalized Differential Transform Method (MSGDTM) in order to compute an approximation to a solution of the model of fractional order. These fractional derivatives are described in a Caputo sense. And a figurative comparison between MSGDTM and a classical fourth-order Runge-Kutta method (RK4) revealed that the proposed method is effective in viruses' counter measures.
Virus Propagation on Time-Varying Networks: Theory and Immunization Algorithms was proposed [16], in order to prevent viruses' epidemic. The model formulates a problem by approximation using Nonlinear Dynamical system and derived a closed formula for the epidemic threshold of time ranging graph under the SIS model as well as exposes the importance of the threshold using heuristic and evaluation method. A Dynamic model of computer viruses was proposed in [18], in order to minimize or prevent risks associated with computer viruses on a network as well as help in understanding the dynamic behavior of viruses on a network environment. The proposed model uses a classical epidemiological model for disease propagations with the use of simple system identification techniques and developed a new model called Susceptible, Antidotal, Infectious, Contaminated (SAIC) model as well as uses a real data about computer virus to validate the proposed model. But fails to consider likely cases of an anti-virus stopped due to drop from a user alertness otherwise known as sensitivity. An analysis of a model of computer viruses spreading via Electronic mail was proposed in [15], in order to discover new approaches on how viruses spread from one PC to another on a network. The proposed model uses a simulation as well as a mathematical approach and clarifies the relevant changes with respect to time of the number of infection, their relationships the number of computers connected, as well as infection and the effect of subjecting viruses spreading by improving a user understanding and knowledge about virus. The proposed model however ignores considering possible re-infection otherwise infection after been immune as a results of anti-virus un-installation or stopped.
Epidemiological Models Applied to viruses in Computer Networks was proposed in [6], to investigate the uses of classical epidemiological model for studying computer viruses' propagation, and gave a detail comparative analysis between computer and population disease propagation by SIR model, modified the models introducing an anti-virus PCs and analyses the possible stability of the disease-free equilibrium position. More so, the proposed model gave a theoretical direction on how to prevent viruses' infection and stress that the number of infected PCs is in respect to a function of time.
Epidemic Thresholds in Real Networks was proposed in [5], to prevent viruses propagating through the network. The model proposed a precise epidemic threshold that may hold irrespective of the network topology, it appropriately captures viruses-propagating properties and developed new immunizations policies while reviling how an epidemic threshold as well as number of infected node decay increasingly with time.
Applying Epidemiology in Computer Virus Prevention: Prospects and Limitation was proposed in [14] to predict the rates as well as the nature of propagation of a computer viruses' infection. It describes the prevalence of computer viruses and explains the importance of epidemiological models in viruses' prevention; The Epidemiological model reveals a well-defined epidemic threshold as well as an imperfect defense against computer viruses which may be highly effective in prevention of their wider spreads if the infection threshold is not exceeded.
On the global stability of an epidemic model of computer viruses was proposed in [19] to leverage the difficulties faced on the network due to virus propagation, the model combines the Lyapunov functions with that of Volterra–Lyapunov matrix classical approach and successfully eliminate the difficulty of determining specific coefficient values, thus, a wider application of Lyapunov functions to dynamic systems which is a basic idea that may lead to more understanding of viruses propagation models.
Numerical Simulation of a Computer Virus Transmission Model using Euler predictor Corrector method was proposed in [20] to understand virus transmission method on the network. This model uses a system of nonlinear ordinary differential equations revealing the transmission of computer virus in a network numerically as well as the Euler Predictor Corrector method; numerical comparisons were carried out with results obtained by Runge–Kutta–Fehlberg method. Hence, the model establishes that Euler Predictor Corrector method may be use in solving mathematical models on the spread of viruses.

3.0 Research Methodology

This section explains how viruses spread as well as infect a user PC and gives a precise explanation on how viruses re-infect already immune PC on the network. Networking is a connection between two or more computers online in order to share data or exchange information. Thus, a PC introduce on the network is likely to be infected since, networking is an age that has come to stay; Viruses are series of program with ability to replicate on the network. Infection may also occur when a user PC comes in contact with an already infected PC on the network.

Viruses Infection/Re-infection

In our proposed model, Viruses propagate when run (executed). Likewise, infection occurs whenever a PC already infected comes in contact with a susceptible PC or are in same group. Re-infection occurs when immune PCs software ((anti-virus) Stopped due to user insensitivity or un-instillation which makes them vulnerable on the

network. A PC becomes immune to viruses whenever an anti-virus software is installed on it and may as well be prone to re-infection if the anti-virus software is uninstalled or stopped, because of a drop-in user alertness otherwise insensitivity. Viruses in a form of files not known by a user may be executed unknowingly. When viruses execute on a susceptible PC it implies that, the viruses can propagate to the most immediate PCs on the group, but when the viruses are latent it implies that, they cannot propagate since latent viruses do not change state. Hence the probability that immune PCs may be re-infected by viruses is 1 - ∝. according to our assumption that immune PCs may be re-infected either due to an anti-virus uninstalled or stopped because of user drop from alertness, the probability that a user may be re-infected if receiving k E-mail messages with viruses on a vulnerable PCs is $(1 - \propto)^{k.}$ That is when viruses are executed at least ones before discovered, and then propagate to the immediate PCs. The immediate PCs may have just received the viruses and are not yet infected otherwise re-infected. In the subsequent stage the PCs may likely transit to re-infected, recovered otherwise immune state. Thus, the re-infected PCs transit to a stage to be recovered otherwise be treated properly before being immune by a reliable, anti-virus software. According to our proposed model, the rules for viruses' re-infection are as follows.

When there are K immune PCs, the state transition probability from the re-infected PCs to the recovered or immune PCs is $(1 - \propto)^{k}$. However, when a PC is removed from the group it implies that individuals from these groups died or were removed. But if there is no immediate PC otherwise adjacent PC in the group k=0 then the susceptible state remains the final state.

3.1 How Viruses Spreads

Computer viruses' spreads using diver's approaches, the methods commonly known are mainly two, which are: Disk drives such as floppy drive, CD and so on as well as the network adapter cards that is network or modem card methods.

Several characteristics exist that differentiate computer viruses with other programming codes. There are several properties that distinguish computer virus from other program code which are replication using self-attachment to innocent executable programs, making one or more copies of self and so on. In which the meaningful programs become infected programs otherwise viruses and then spreads to immediate PCs.

Viruses may also be activated under certain conditions as well as make some malicious actions to a host computer user. Most of the computer viruses contain a destructive series of information commonly called "payload" which can be triggered by the arrival of a particular data or action performed by a user. The effect of these payloads can be disastrous in many cases which may likely cause a permanent loss of information or data as well as a hardware component. A typical viral infection is explained in the following Algorithm **1.**

Algorithm 1: This explains the step by step procedure of how viruses propagate from one PC to another on the network as seen bellow.

Algorithm 1:

Step 1: *StartExecution*;

Step 2: *if an– Executable file –is found* ;

else

Step 3: *the files– contain– virus –codes*;

endif found

Step 4: *elseif virus –codes– not found*;

add– a –copy– of virus– codes

on–un inf *ected files*&*execute*;

Step 5: *end*

We derive a mathematical analysis of how viruses spread algorithmically, as well as simulation, according to our proposed model in section 4. The spread of viruses is presented in a one-dimension array, as well as a precise characteristic of a number of re-infections are justified.

In our simulation, the effects of preventing the spread of viruses to increasing awareness as well as the knowledge of users against viruses as well as the effects of preventing the spread of viruses by means of a software (anti-virus) were detailed in a networking environment with more than three (3) connections per computer systems on a range by using a specific one-dimensional array with periodic boundary conditions and then.

We propose a SiIMRiIM model for computer viruses counter measures; in our model, we propose that computers even after been immunized may be re-infected with viruses due to a slight drop from a user alertness resulting to a stop state or as a result of an anti-virus software being uninstalled from a user PC(s) completely.

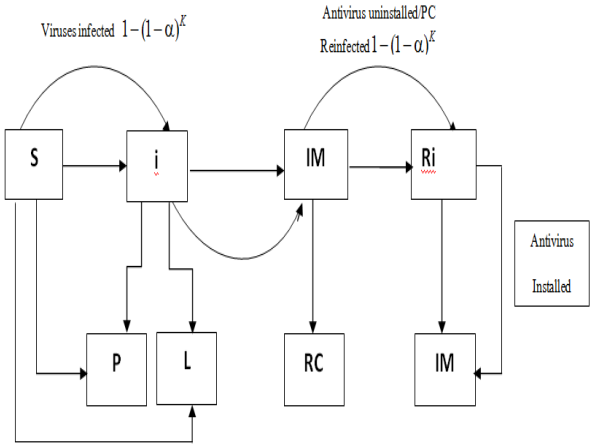
4.0 Evaluation and Results

In this section, we present our findings as: firstly, our proposed model, secondly our mathematical model and then simulation. As seen below. The proposed model Comprises of five populations which sum up the name SiIMRiIM as seen bellow. This model shows a clearer state transition from one state of a user PC to another. It describes an appropriate approach addressing cases of viruses' re-infection that may likely exist as well as proffer solution to already re-infected PCs.

Viruses at execution state in P $(1-\alpha)^{k}$

and viruses at latent state in L

Figure1. Shows a Diagrammatic model $(1-\alpha)^k$ l of PCs state transitions seen bellow.



Note: Table 1 shows notations used in figure 1 model and their meaning as seen bellow.

susceptible	infected	Immune	Re-infected	propagate	latent	recovered
(S)	(i)	(IM)	(Ri)	(P)	(L)	(RC)

Mathematical model

In our mathematical model, we assume a network of computers with at least two users connected, that is k=2. These computers originally were immune with anti-virus software, but subsequently the anti-virus software was uninstalled. Hence, the PC(s) become vulnerable and prone to viruses re-infection. Furthermore, the anti-virus software of the remaining PCs is stopped due to user insensitivity or a drop from user alertness. Therefore, these computers are prone to re-infection, and a computer that is said to be re-infected is known as the "infection source computer": we use an infinite one dimensional array to consider the state transitions of PCs in stages. We consider the state of all PCs at step q precisely see figure 2 it shows the state transition, step one to q in which four systems are connected together, the viruses propagates 1 computer in their respective direction for each transition. Therefore, PCs that may be re-infected at q+1 from q were separated by q units from the infection source computer. Likewise, q is the number of transitional steps and distance as well between the propagate PC and the infection source PC.

∞ …	q+1	q	q-1	...	2	1	0	1	2	...	q-1	q	q+1	… ∞
			(1 - ∝)								(1 - ∝)			

Figure 2. Shows a state transition of PCs in stages seen above.

Our model considers the q[th] PC on both sides of infection referred as PC_q. Therefore, as the expected values for the number of infection at q are equal to I_q this is express as bellow:

$$I_q = I_{q-1} -_p I_{q-1} + \Delta I^+_{q-1} - \Delta I^-_{q-1} \quad \text{Equation (1)}$$

$$= (1-P)^q I_0 + \sum_{j=0}^{q-1} (1-P)^{q-1-j} (\Delta I^+_j - \Delta I^-_j) \quad \text{Equation (2)}$$

The four conditions on the left hand side of equation one (1) signifies the numbers of infection at step q-1, the number of transition from infected state to immune state when a user discovers the viruses activity, the number PCs re-infected by a propagating viruses as well as number of transition to a safe state called the "immune"; when the viruses are discovered if received on infected PCs are ΔI^+_q and ΔI^-_q mathematically coupled as:

$$\Delta I^+_q = 2(1-\alpha)^{q+1} \quad \text{Equation (3)}$$

$$\Delta I^-_q = 2(1-\alpha)^q (1-P)\alpha \quad \text{Equation (4)}$$

Our assumptions are:

$$\Delta I^-_0 = 0 \quad \text{Equation (5)}$$

$$\Delta I^-_1 = 1-(1-\alpha(1-\alpha)(1-P))^2 \quad \text{Equation (6)}$$

ΔI^+_q In equation 3, is our expected value for the number of re-infection between them, q and q+1.

$(1-\alpha)^{q+1}$ Implies the probability of continuous re-infection from one PC to another that is from PC_1 to PC_{q+1}. In equation 4, ΔI^-_q implies expected values for the number of re-infections in between q and q+1. $(1-\alpha)^q(1-P)\alpha$ implies the probability that a user on PC_{q-1} may discover viruses after receiving messages from PC_q if PC_q and PC_{q+1} are already re-infected at step 0^{th}.

If the PC has not received a copy of viruses code it will remain $\Delta I^-_0 = 0$. In the initial step, PC_0 may receive viruses from PC_1 on each side. ΔI^-_1 = The probability of receiving and discovering a virus from pc_1 on minimum of one side. . $\alpha(1-\alpha)(1-P)$ = The probability of discovering viruses if received from pc_1 .Substituting equation 3 with 6 into equation 2, and we simplified our results we obtain

$$I_q = (1-P)^q I_0 + (1-P)^{q-1} \Delta I^+_0$$

$$+(1-P)^{q-2}(\Delta I^+_1 - \Delta I^-_1)$$

$$+2(1-2\alpha+P\alpha)\frac{(1-\alpha)^2(1-P)^{q-2}-(1-\alpha)^q}{\alpha-P} \quad \text{Equation (7)}$$

Our earlier assumptions are:

$$I_0 = 1$$

$$I_1 = (1-P)I_0 + \Delta I^+_0$$

$$I_2 = (1-P)^2 I_0 + (1-P)\Delta I^+_0 + \Delta I^+_1 - \Delta I^-_1 \quad \text{Equation (8)}$$

$$I_2 = (1-P) + \Delta I^+_1 - \Delta I^-_1 \quad \text{Equation (9)}$$

More so, our results of the mathematical model in equation 7 were compared with that of the simulation. A probability of $\alpha = (0.1/0.01)$ and a probability that P = (0.02/0.2) combined together, as well as a range of re-infection were computed significantly up to exactly 500 steps. In our simulation, the total number of PCs was also set to 400, as well as the number of connections was in two respectively, per a PC. The plot in **figure 3** represents an average of over 1000 simulation run using same parameter sets. In the plot the horizontal axis represents the time (t) steps while vertical axis is the assumed numbers of re-infected PCs.

The top left symbols as well as figures are our simulation (S) and mathematical (M) results. The values after symbol S, M are α and P respectively. Our results proved that the proposed mathematical model as well as that of the simulation agree except in cases where P = (0.01, 0.0), their differences rises with respect to time. In our mathematical model the numbers of PCs were not limited so that we obtain a maximum number of re-infection cases while in the simulation the number of PCs were limited, as such, the number of re-infection was subjected by the number of user PCs. Furthermore, the difference in the number of re-infections rises with time.

The result in which number of re-infections were subjected by a particular number of PCs is called size effect (s). Finally, we have proved that a simulator with α equal to (0.01) as well as P = (0.0) their differences ranges within two (2), whenever a total number of PCs were raised from 400 to 1000. And then we estimated the limits characteristics of the number of re-infected PCs.

Hence, if the limit $q \to \infty$ it implies that equation 7, is used. And we have

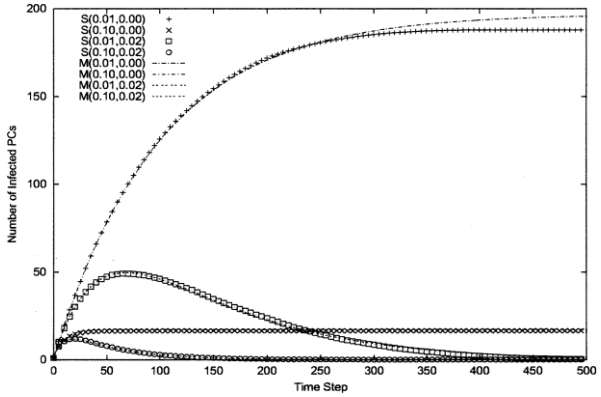


Figure (3). Shows a plotted graph with an average number of infected user PCs against time with a simulation run as well as a mathematical model

$$I \propto = \lim_{q\to\infty} I_q = \int^0 \frac{(\alpha^2-\alpha+1)(\alpha^3-\alpha^2-\alpha+2)}{\alpha}$$

$$(P \supset 0) \text{ and } (P \equiv 0) \quad \text{Equation (10)}$$

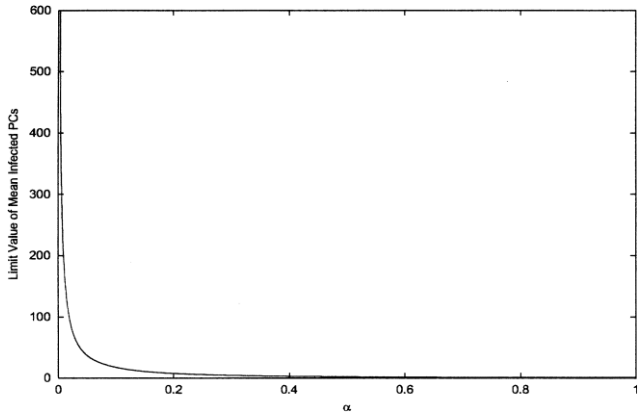


Figure 4. Shows the Limits value of the mean infected otherwise re-infected PCs ($I\infty$) against the Probability I_∞ of discovery when receiving viruses.

Whenever viruses' payloads are run, if $P \supset 0$, it is clear, according to equation 8, that viruses will ultimately die. After being re-infected, if the viruses don't have payload $P \equiv 0$, the limits value may be different depending on α, their differences in P can also be confirmed in figure 3. When P=0, the exact limit number of re-infection is also shown by the curve line in figure 4 above. As α varies, the number of re-infection rises faster according to figure 4, as α crosses the range of 0.05 as well as approach 0.0.

This paper considers a mathematical model concept with two connections, since mathematical models with two or more connections are much difficult to formalize using our method described here, that is because changes in the number on re-infection with each state depends not just on the number of PCs in the propagating state but, on their

respective arrangement, and the number for the arrangement rises as the number of connections rises. Both mean field as well as pair approximation may be used, but in our model the likely probability of re-infection depends on the way the PCs that propagate (infection source PC) are arranged with other susceptible PCs on the network, thus approximation cannot be used.

5.0 Conclusion

An enhance model for computer viruses Counter measures have been proposed. These model employs a systematic transition stages of development and provides counter measures for viruses when infected otherwise re-infection occurs and propose an algorithm for viruses 'propagation in order to improve on a user understanding of viruses on the network and prevent or minimize virus propagation. The model has a precise implementation procedure, and it significantly helps increase user knowledge and understanding the dynamic behaviors' of viruses, our simulation and mathematical results proved that the propose model significantly enhances viruses counter measures.

References

[1] A. H. Handam, A.A. Freihat**,** A new analytic numeric method solution for fractional modified epidemiological model for computer viruses. Application and applied mathematics: an international journal (AAM) vol. 10, issue 2 (December 2015), pp. 919-936.

[2] D. Chakrabarti, Y. Wang, C. J. Leskovec, and C. Faloutsos, 2008. Epidemic thresholdsDepartment of Computer Science University of Auckland.

[3] M. Draief, A. Ganesh, L. Massouili Thresholds for virus spread on networks. Annals of Applied Probability 2008; 18(2): 359–78.

[4] B. Drossel, F. Schwabl, Formation of space-time structure in a forest-fire model. Physica A 1994; 204:212–229.89.

[5] D. Chakrabarti, Y. Wang, C. Wang, J. Leskovec, and C. Faloutsos. Epidemic threshold in real networks. ACM Transactions. Information. System. Security. 10, 4, Article 13 (January 2008), 26 pages.

[6] J. Roberto, C. Piqueira, B. F. Navarro and L. Henrique, A. Monteiro, Epidemiological Models Applied to Viruses in Computer Networks Journal of Computer Science 1 (1): 31-34, 2005, ISSN 1549-3636.

[7] K. JO, White SR, Chess DM. Computers and epidemiology. IEEE Spectrum 1993:20–6.

[8] K. WO, Mc Kendrick AG. Contributions of mathematical theory to epidemics. Proceedings of the Royal Society of London – Series A 1933;141:94–122.

[9] S. Lynch, BK Mishra, D. Saini, Mathematical models on computer viruses. Applied Mathematics and Computation 2007; 1.187(2):929–36.

[10] N. MEJ, S. Forrest, J. Balthrop, Email networks and the spread of computer viruses. Physical Review E 2002; 66:035101-1–035101-4.

[11] C. Piqueira, BF Navarro, LHA Monteiro Epidemiological models applied to viruses in computer networks. Journal of Computer Science Jan.–Mar. 2005; 1(1):31–4.

[12] Y. Sengoku, E. Okamoto, S. Hattori, Computer virus diffusion and extinction evaluation in networks with vaccine-free nodes. IPSJ J 1998; 39:818–825.

[13] Symantec. Understanding heuristics: Symantec's bloodhound technology. 1997.

[14] Weiguo Jin.Applying Epidemiology in Computer Virus Prevention: Prospects and Limitations Department of Computer Science University of Auckland, 2000.

[15] T. Okamoto, and Y. Ishida, An Analysis of a Model of Computer Viruses Spreading via Electronic Mail, Systems and Computers in Japan, Vol. 33, No. 14, 2002.

[16] B.A Prakash, H. Tong, N. Valler, M. Faloutsos, and C. Faloutsos,Virus Propagation on Time-Varying Networks: Theory and Immunization Algorithms. Department of Computer Science, University of California – Riverside, 2010.

[17] Systems with applications using MATLAB. Boston: Birkhuser; 2004.

[18] J. R.C. Piqueira, A. A. de Vasconcelos, E.C.J. C. Gabriel, V. O. Araujo, Dynamic models for computer viruses computers & s e c u rity 2 7 (2 0 0 8) 3 5 5 – 3 5 9.

[19] M. R. Parsaei, R. Javidan, N. S. Kargar, H. S. Nik, On the global stability of an epidemic model of computer viruses, Theory Biosci. DOI 10.1007/s12064-017-0253-2 2017.

[20] C. Onwubuoya, S.T. Akinyemi, O.I. Odabi, G.N. Odachi Numerical Simulation of a Computer Virus Transmission Model using Euler predictor Corrector method, International Digital Organization for Scientific Research ISSN: 2550-7931 IDOSR JOURNAL OF APPLIED SCIENCES 3(1) 16-28, 2018.