iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 6 **Issue:** VII **Month of publication:** July 2018

DOI: http://doi.org/10.22214/ijraset.2018.7120

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue VII, July 2018- Available at www.ijraset.com

Modelling the Spread of Computer Virus under Users Computer Security Behaviour: An Agent-Based Model

Esmael V. Maliberan[1]
[1]*Graduate Studies Department, Surigao del Sur State University*

Abstract: ***This study aimed to investigate the effect of Users computer security behaviour on the spread of computer viruses. This paper used the AIDS model found in Net logo which characterized the propagation of virus in order to predict future threats and its rate of infection over a period of time. Findings revealed that computer virus infection was largely dictated by the behaviour characteristics of the computer users. Such behaviour characteristics may deter to facilitate the spread of the virus. In turn, informed users were more likely to exercise caution and observe practices that stop the spread of the virus.***
Keywords: Computer virus, Users computer security behaviour, NetLogo, AIDS model

I. INTRODUCTION

Computer virus is an executable code able to reproduce itself which can destroy the operating system and files of a computer [1]. It affects efficient performance and production of the business firms and other economic entities. Not only these entities are affected by computer virus but also those individuals having important files kept in the computer. In this study, the spread of computer virus is modelled on the basis of the users' computer security behaviour.

Employees in a certain organization play an essential role in keeping their computer free from virus infection in order to maintain the integrity and safety of the information. It is somewhat significant to consider what influences a user to observe computer security procedures.

To further improve the security level, users have to make responsive choices to act in accordance with the management's security policies and implement computer security behavior. Thus, organizations have been employing security trainings and awareness programs to educate users [2].

II. PROBLEM STATEMENT

This study determines the effect of Users' computer security behaviour towards the spread of computer virus. It is sought to answer the following questions:

A. What is the rate of infection of a computer owned by a user who rarely transfers files from outside source and does not update his antivirus software regularly?
B. What is the rate of infection of a computer owned by a user who sometimes transfers or copies files from outside source and update his antivirus software regularly?
C. What is the rate of infection of a computer owned by a user who frequently transfers or copies files from outside source and update the antivirus software regularly?
D. How long will it make 80% rate of infection for a user who frequently transfers or copies files from outside source and is not updating his antivirus software regularly?
E. What is the effect of transferring of files to a non updated antivirus software installed in a computer?

III.OBJECTIVES

A. The Objectives of the Study are as Follows

1) To determine the rate of infection of a computer owned by a user who rarely transfers files from outside source and does not update his antivirus software regularly;
2) To determine the rate of infection of a computer owned by a user who sometimes transfers or copies files from outside source and update his antivirus software regularly;
3) To determine the rate of infection of a computer owned by a user who frequently transfers or copies files from outside source and update his antivirus software regularly;

4) To determine how long will it make 80% rate of infection for a user who frequently transfers or copies files from outside source and is not updating his antivirus software regularly; and

5) To determine the effect of file transfer to a non updated antivirus software installed in a computer.

IV. RELATED LITERATURE

The framework used for this study is the AIDS model found in the NetLogo. NetLogo is a multi-agent programmable modelling environment. It is used by tens of thousands of students, teachers and researchers worldwide [3]. It also powers HubNet participatory simulations. Indeed, it is authored by Uri Wilensky and developed at the Center of Connected Learning and Computer-Based Modelling [4].

Furthermore, there are research studies that model the spread of computer virus in order to predict future threats and the rate of infection in a machine over a period of time. An example of this study is the proliferation of computer virus in human intervention: A dynamical model by [5]. The study scrutinized the proliferation behaviour of computer virus in human intervention. A dynamical model recounting the spread of computer virus, in which a vulnerable computer can be recovered directly and an infected computer can be vulnerable directly. During a qualitative analysis of this model, findings revealed that the virus-free stability is globally asymptotically stable when the basic reproduction number R0 $\leq$1, whereas the viral equilibrium is globally asymptotically stable if R0 >1. Based on the findings and a parameter analysis, several suitable methods for eliminating the propagation of computer virus across the internet are suggested.

In an organizational context, a study by [2] regarding users' computer security behaviour in a Health Belief perspective. It explored what impact a user to exercise computer security. The study utilized the Health Belief Model, adapted from the healthcare literature to study the computer behaviour of the users. The model was validated through the use of survey data from 134 respondents. Findings revealed that perceived benefits, perceived susceptibility, and self efficacy are determinants of email related security behaviour. Perceived asperity moderates the effects of general security orientation, perceived benefits, cues to action, and self-efficacy on security behaviour.

Reference [6] explained the factors affecting the propagation of computer viruses in removable storage devices. It offered a way other than the internet for the proliferation of computer virus. Nevertheless, almost all earlier models of viruses deemed that internet was the source of the virus spread, ignoring the removable device route at all. In this study, a novel propagation model of computer viruses, which integrate the effect of removable device, was recommended. Moreover, the model divulges a distinctive virus stability, which is shown to be globally asymptotically stable. The result means that any attempt to eliminate viruses failed to succeed. By scrutinizing the relevant influences of system factors, a lot of guidelines are suggested so as to limit the quantity of the infected computers to an acceptable threshold.

Outbreak dynamics of computer viruses is a promising discipline aiming to recognize the way that computer viruses propagate on computer networks. Meanwhile, [7] intended to create a series of realistic endemic models of computer viruses. Initially, a close examination of some frequent types shared by all usual computer viruses clearly tells the defects of prior models. Afterwards, a generic epidemic model of viruses named as the SLBS model, was recommended. Certainly, various generalizations of the SLBS model are recommended.

Reference [8] examined the results of infected removable storage devices and external computers on the spread of computer viruses. Because of this, a new compelling model of four sections was proposed. The investigation of the model revealed that the distinctive equilibrium is globally asymptotically stable. This result is well fitting for numerical operation. An interpretation of the influences of infected removable storage devices and computers was also contained. Besides, it was found out that (1) removable storage media and external computers that were infected by the virus can both accelerate it spread; (2) infected removable storage devices can cause a greater risk than infected computers.

In order to curb the spread of computer virus on the Internet, a new Susceptible-Infected-External (SIE) model, a study of [9], which considered the impact of external computers on virus propagation behaviour, was put forward. This model puts external and internal computers as a whole to study. By applying dynamical stability theory, the existence and global stabilities of virus-free and viral equilibrium were fully studied. Based on the further analysis of numerical simulation results and system parameters, some effective measures controlling the prevalence of virus were suggested.

V. METHODOLOGY

The method that is used in this study is both modelling and simulation which is anchored in the AIDS model found in NetLogo Programmable Software.

A. The model relies on the Following Basic Assumptions

1) External source of files (internet, removable storage device) can be the source of computer virus.
2) The more transfer of files from external source the more chances the computer will be infected by computer virus.
3) Once the computer virus begins to infect the file, it will infect other files in the system.
4) Computer is vulnerable to virus infection once antivirus installed is not updated.The model then simulates the scenario on how the computer virus enters the computer based on the users' computer security behaviour. This scenario is systematically drawn below:

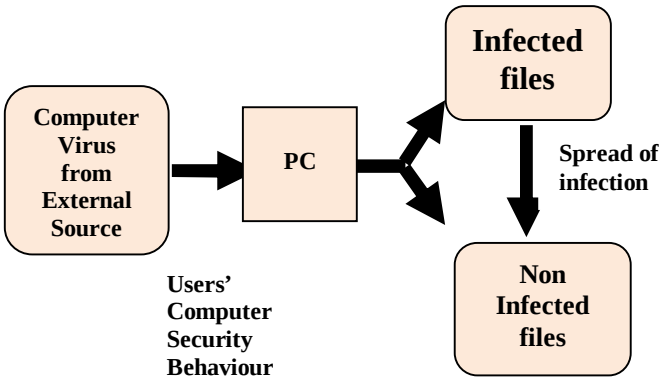


Fig. 1 Schematic Diagram of the Scenario

B. Parameters

The present scenario of computer virus spread under user behaviour is represented through the model which is subject of the algorithm that will be coded based on the following parameters of the study. These are:

1) File size in GB.
2) Ave. Frequency of transfer of files from external source
3) Ave. length of time file which is in contact with external source
4) Ave. frequency of updating antivirus
5) Frequency of full File Scan

This study make use of the existing AIDS model of Uri Wilensky (2007), found in the net logo models library with the following changes in the parameter definition, which is shown in Table 1.

Table I. Analysis on the Parallelism of Parameters Used in Different Model

A. Parameters in AIDS Model	*B.* Parameters in Computer Virus Model
Initial-People	File size in GB
Average Coupling Tendency	Ave. Frequency of transfer of files from external source
Average Commitment (weeks)	Ave. length of time file which is in contact with external source
Average Condom Use	Ave. frequency of updating antivirus
Average Test Frequency (0.00 times/year)	Frequency of full File Scan

C. PROCESS and OUTPUT

The parameters defined are utilized and processed using a Net Logo Programmable Software to the macro-behaviours driven the micro-attributes of the agents.

.

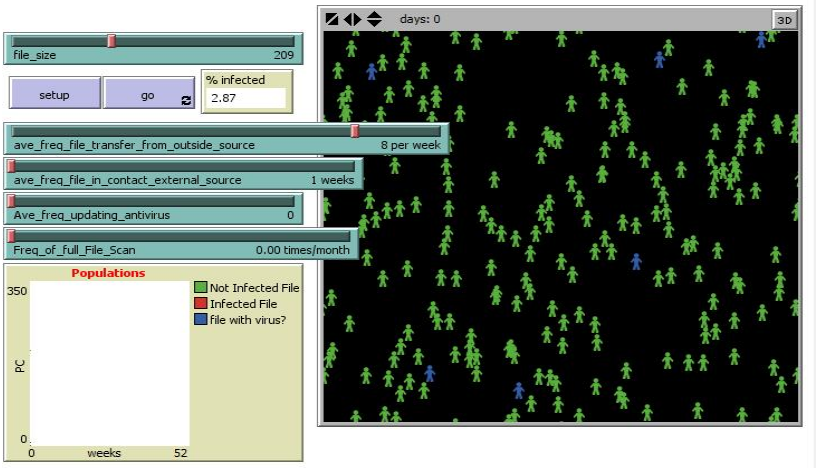


Fig. 2 Sample Screen Shot of the model

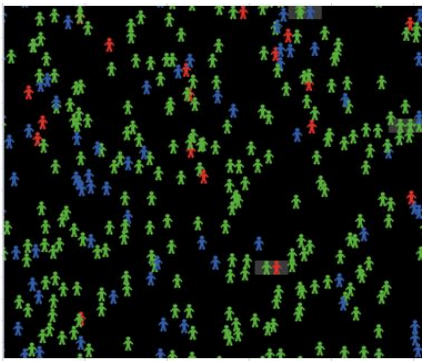
The result of simulation is recorded by adjusting the slider of each parameter (user's computer security behaviour). Trials were recorded and other simulations were used to answer key questions in the statement of the problem.

VI. RESULTS AND DISCUSSIONS

Based from the result of trials from Table II through Table IV, it is found out that the spread of computer virus is slower if the user will always update the antivirus software installed in his computer. However, the rate of infection becomes faster once the user will not update his antivirus software. In other words, the spread of computer virus is directly proportional to the average frequency of file transfer from outside source and none updating of antivirus in a computer. Additionally, even if there is a frequent transfer or moving of files from outside source (e.g. removable disk, internet) as long as the user will update the antivirus software installed in his/her computer, there is a lesser probability of virus attack.

Table II. Simulation Results of the Rate of Infection for a Rarely Transfer of File from Outside Source

Average frequency of file transfer from outside source Rarely (n=2/10)	Trials 1.00	2.00	3.00	4.00	5.00	6.00	7.00	8.00	9.00	10.00	Average
Always Updating Antivirus	3.33	3.00	4.67	2.67	3.67	2.67	2.67	3.33	2.67	4.00	3.27
Sometimes Updating Antivirus	28.67	16.33	4.33	30.67	19.67	12.00	23.00	32.33	12.33	27.33	20.67
Never Updating Antivirus	25.67	35.67	22.33	14.67	27.33	13.00	24.00	9.00	31.67	36.00	23.93



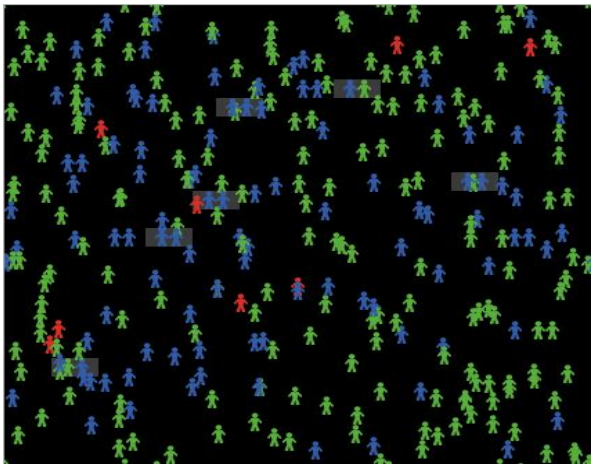
Legend: Green- file that is not infected
Red-Infected File
Blue-file at risk

Fig. 3 Typical output of the system for a rarely transfer of file from outside source and never updating an antivirus.

Table III. Simulation Results for Sometimes Transferring of Files from External Source.

Average frequency of file transfer from outside source occassionally (n=5/10)	Trials										Average
	1	2	3	4	5	6	7	8	9	10	
Always Updating Antivirus	4.67	3.33	3.00	3.33	5.00	6.67	2.67	3.67	4.00	5.00	4.13
Sometimes Updating Antivirus	71.00	83.33	73.33	65.67	64.00	69.00	68.00	65.00	69.33	70.00	69.87
Never Updating Antivirus	81.00	70.00	80.00	70.00	67.00	85.33	80.00	77.00	81.00	85.00	77.63

]

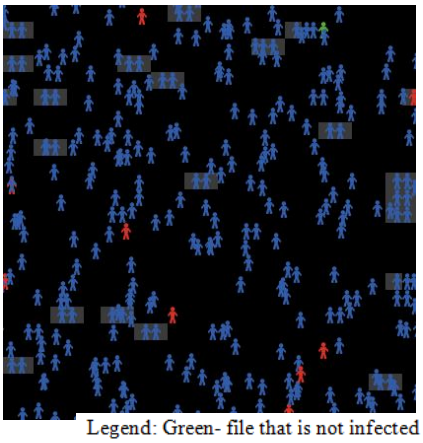


Legend: Green- file that is not infected
Red-Infected File
Blue-file at risk

Fig. 4 Typical output of the system for an occasional transfer of file from outside source and sometimes updating an antivirus.

Table IV. Simulation Results of the Rate of Infection for a Frequently Transfer of File from Outside Source

Average frequency of file transfer from outside source frequently (n=8/10)	Trials										Average
	1	2	3	4	5	6	7	8	9	10	
Always Updating Antivirus	7.00	3.33	5.00	3.00	5.67	5.67	5.00	2.67	4.67	6.67	4.87
Sometimes Updating Antivirus	99.67	99.67	99.67	100.00	99.67	100.00	99.00	99.67	99.67	99.33	99.64
Never Updating Antivirus	100.00	99.67	99.67	99.67	100.00	100.00	100.00	100.00	99.67	99.67	99.84



Legend: Green- file that is not infected
Red-Infected File
Blue-file at risk

Fig. 5 Typical output of the system for a frequently transfer of file from outside source and sometimes updating an antivirus.

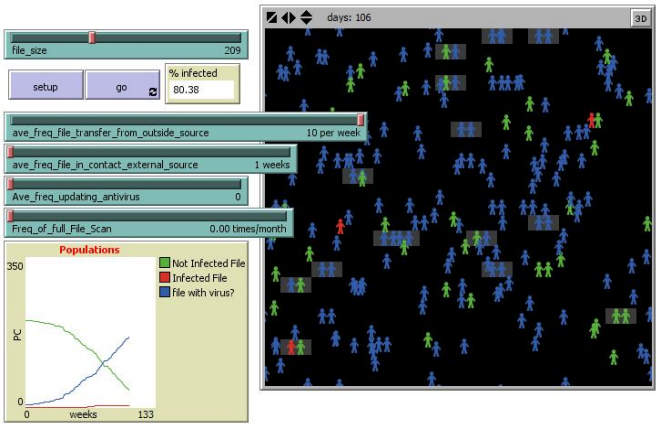
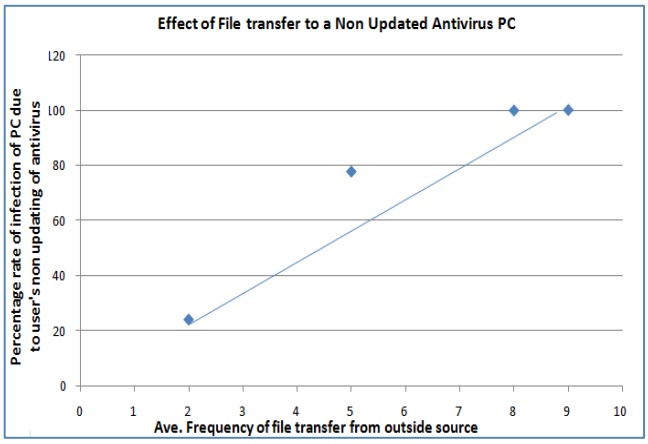


Fig 6. 80% rate of infection for a user who frequently transfers or copies files from outside source and is not updating his antivirus software regularly



$Y = 10.9x + 10.1$

$R^2 = 92.0\%$

Fig. 7 The Effect on the ave. frequency of transferring of files from external source.

VII. CONCLUSION

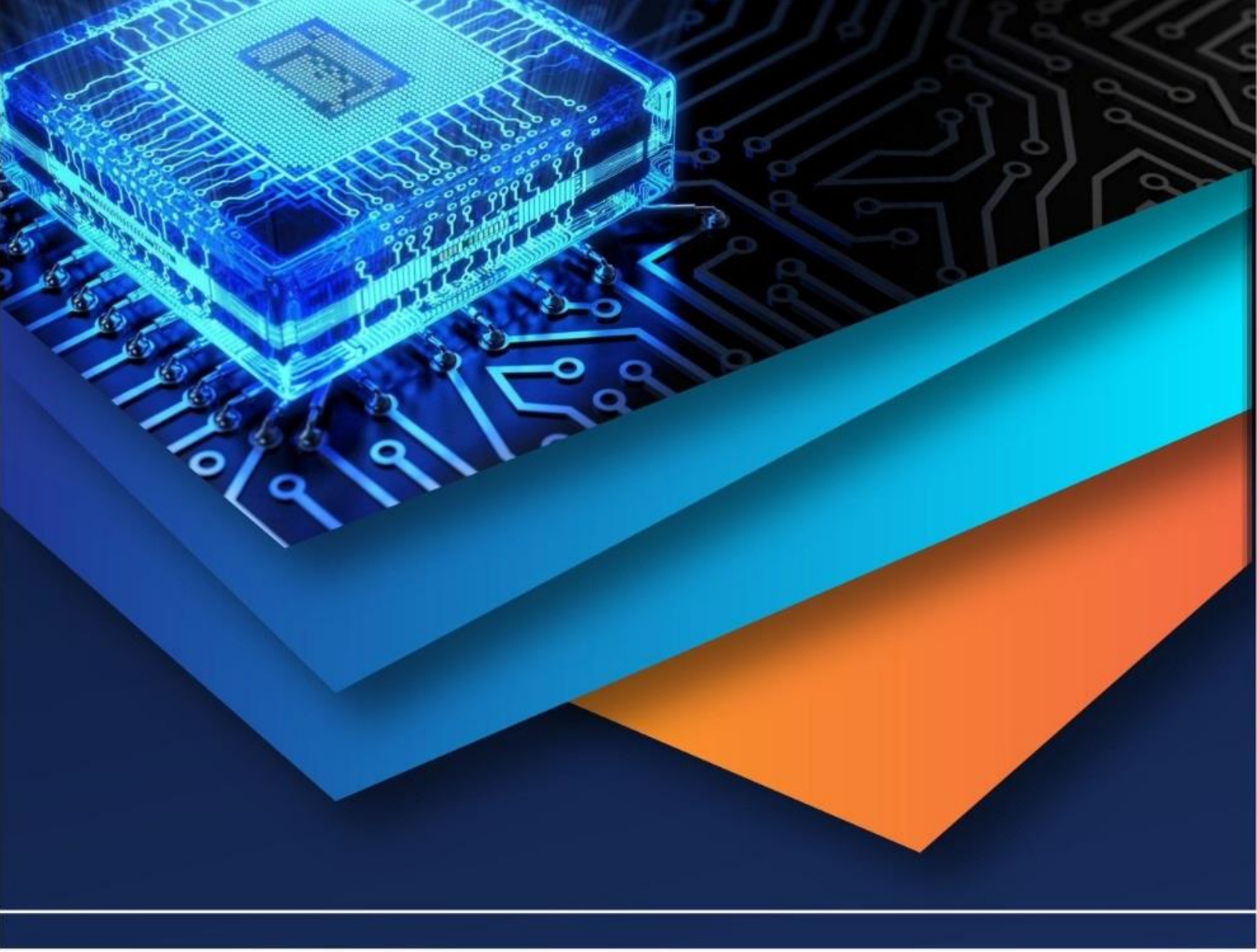
The spread of computer virus was due to user's failure to update antivirus software installed in a computer. Therefore, computer virus infection is largely dictated by the behaviour characteristics of the computer users. Such behaviour characteristics may deter to facilitate the spread of the virus. In turn, informed users are more likely to exercise caution and observe practices that stop the spread of the virus.

VIII. RECOMMENDATIONS AND FUTURE WORKS

A user must always update the antivirus installed in his/her computer at all times. Effective antivirus software that has auto update and auto block feature must be considered in choosing antivirus software. The author recommends for the next work to model and simulate the spread of computer virus on complex network.

REFERENCES

[1] Computer Viruses", 123helpme.com, 2016. [Online]. Available: http://www.123helpme.com/computer-viruses- view.asp?id=158564. [Accessed: 20- Jul- 2016].
[2] Ng, A. Kankanhalli and Y. Xu, "Studying users' computer security behavior: A health belief perspective", Decision Support Systems, vol. 46, no. 4, pp. 815-825, 2009.
[3] U. Wilensky, "NetLogo", NetLogo, 1999. [Online]. Available: https://ccl.northwestern.edu/netlogo/. [Accessed: 20-Jul-2016].
[4] U. Wilensky and W. Rand, An Introduction to Agent-Based Modelling: Modelling Natural, Social, and Engineered Complex Systems with Netlogo. Cambridge, Massachusetts, London, England: The MIT Press, 2015.
[5] C. Gan, X. Yang, W. Liu, Q. Zhu and X. Zhang, "Propagation of Computer Virus under Human Intervention: A Dynamical Model", Discrete Dynamics in Nature and Society, vol. 2012, pp. 1-8, 2012.
[6] Yang and X. Yang, "The spread of computer viruses under the influence of removable storage devices", Applied Mathematics and Computation, vol. 219, no. 8, pp. 3914-3922, 2012.
[7] X. Yang and L. Yang, "Towards the Epidemiological Modeling of Computer Viruses", Discrete Dynamics in Nature and Society, vol. 2012, pp. 1-11, 2012.
[8] Zhang, "Modelling the Spread of Computer Viruses under the Effects of Infected External Computers and Removable Storage Media", IJSIA, vol. 10, no. 3, pp. 419-428, 2016.
[9] J. Chen, "Propagation of Computer Virus under the Influence of External Computers: A Dynamical Model", J. Inf. Computer. Sci., vol. 10, no. 16, pp. 5275-5282, 2013.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY