Journal of Engineering and Applied Sciences 14 (10): 3266-3270, 2019
ISSN: 1816-949X

System Dynamic to Analyze the Effects of Worms and Viruses on Computer Efficiency

[1]Naji Mutar Sahib and [2]Rouwaida Hussein Ali
[1]Department of Computer Science, Collage of Science,
[2]Collage of Engineering, University of Diyala, Diyala, Iraq

Abstract: Computers worms and viruses have harmful effects on the performance of the computers, computer worms are calculations that live on one or more machines. The individual computers programs are defined as the worm segments, the mechanism of the worm is to gather and maintain the worm segments, whilst user programs that are real then built on top of this mechanism. The aim of this study is to analyze the effect of the worms and viruses on the computer using simulation technique which is system dynamic in terms of tasks, the results show that The effect of the viruses and worm as viruses cause speed to be slow and the work cause the network to be disabled and both lead to cause performance error and thus, the effect of worms and viruses on the tasks performed by the computer will be less as it cause computer disable of the work and also slow the speed of it.

Key words: Worms, viruses, disable, speed, system dynamic, network

INTRODUCTION

The term security refer to the defense against attack of the malicious by outsiders (and by insiders). Statistically, inside sources attacks are many. Security, also include controlling theerrors effects and failures of equipment. Anything that can defend against an attack will possiblystop random misfortunes, too (Stallings, 2003).

The term computer virus become familiar in the past years. The computer viruses have been heard by everyone even those who don't know how to use a computer through Hollywood movies like Independence Day or Hackers. Newspapers and International magazines frequently have virus scares as leading stories. There is no doubt that our culture is captivated or frustrated by the possible danger of these computer viruses (Li, 2003).

A computer virus is a kind of malicious software program ("malware") that when performed, repeated itself by adjusting other computer programs and introducing its own code (Stallings and Brown, 2012). An operation system program for personal computer that infected operating system versions found in on diskette that include an attractive game represent an example of computer viruses. For the game to work, the diskette should be used to boot the computer, irrespective of whether the computer comprises a hard disk with its private copy of the (uninfected) program of operating system (Wack and Carnahan, 1989).

Computer worms is daunting and critical task. The damage possible from computer worms has enlarged instraight relationship to the significance of legitimate software in our lives. The programmers of security professionals and malicious worm fight have been increasingsteadily as has the inventiveness of these programmers (Li and Knickerbocker, 2007).

A computer worm is a separate malware computer program that duplicates itself to extend to other computers. Frequently, in order to spread it uses a computer network, depending on failures of security on the target computer to admission it. At least some harm found in the network that causes worms, even if only bandwidth is consuming but viruses almost always files are corrupted or modified on a targeted computer (Barwise, 2014). This study describes the behavior of the viruses and worms in the computer in terms of tasks using technique system dynamic, so, dynamically follow their behavior in the computers.

Literature review: Consumer reports in the USA survey in the internet survey third annual Statein 2006 in the past 2 years, approximately US$8 billion was lost by Americans due to computer viruses, spyware and phishing scams. About US$5.2 billion needed to replace the computer and employ technical support people to fix computer due to the effect of viruses (Fox, 2006).

A common phenomenon in today's internetare worms and source damages about tens of billions of dollars to

Corresponding Author: Naji Mutar Sahib, Department of Computer Science, Collage of Science, University of Diyala, Diyala, Iraq

businesses every where in the world every year. A sensitive information is stolen, files are removed, network slow down, use the infected hosts touse the infected hosts to introduce other types of attacks hence compromise the systems and in spite of a large research has been done, protection against worm attacks stays largely an open problem and attack of worm is still anenormous threat to the communities of network for the following causes: first with the growth of applications of network, worms can take various method to spread themselves rapidly. Second, the speed of worms spreading is much more rapidlythan human beings can manually reply (Tang *et al*., 2009).

Computers worms and viruses have harmful effects on the performance of the computers, computer worms are calculations that live on one or more machines. The individual computers programs are defined as the worm segments; the mechanism of the worm is to gather and maintain the worm segments, whilst user programs that are real then built on top of this mechanism (Cohen, 1991).

A network worm takes the same features as the virus computer: a mechanism of replication, probably an activation mechanism and an objective. The mechanism of replication usually executes the following functions: seeks to infect other systems by examining tables of the host or comparable repositories of remote system addresses. Connection creation a with a remote system, probably by logging in as a user or using a mail facility or capability of remote execution (Stallings and Brown, 2012). This study aims at analyzing the worms and viruses effect using a sophisticated technique which called system dynamic.

MATERIALS AND METHODS

In this study, the effect of various and worm take from a questionnaire that was given to the programmer, a system dynamic was used which is a simulation technique system dynamics is a methodology of dynamically complex systems studying and management simulation model building (Ford *et al*., 2004). System Dynamics (SD) development wasin the late of 1950's for industrial systems analysis (Forrester, 1961). SD has been applied successfully to problems, ranging from social, environmental and industrial project management systems (Fig. 1). The steps of system dynamic as follows (Martin and Sterman, 2017).

Identifying the problem: Once the essence of the problem is identified, a description should be completed, depending on the expert's knowledge on the subject,

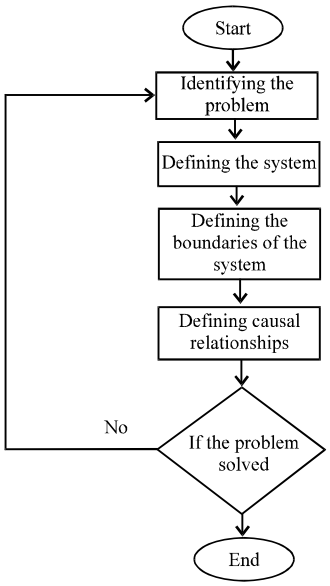

Fig. 1: System dynamic steps

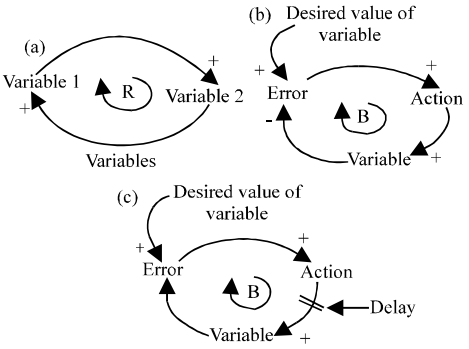

Fig. 2: Component of the system dynamic: a) A rainforcing loop; b) A balancing loop and c) A balancing loop with delay

basic documentation, etc. This phase result must bean initial perception of the elements that problem has been bearing, the hypothesized relationships between them and behavior of their history (Fig. 2).

Defining the system: When we analyze a system we usually focus merely on the characteristics of its constituent elements. However, in order to understand the functioning of a complex system, we must focus also on the relationships that exist between the elements which form the system.

The boundaries of the system: The system should contain as few elements as possible while providing a simulation which will genuinely permit the person to decide the most efficient solution of the possible courses of action that has been studied to the problem. The models are

communally small to start with few elements. They are then extended and perfected. After that, elements which don't play a pivotal part in the problem are deleted. During the model construction, there are many phases of extension and simplification in which elements are subtracted and added.

Causal relationships: The models the system dynamics are causal relationships of reinforcing (positive) and balancing (negative). The meaning of the relationship of the positive causal that if variable increase or decrease that lead that variable B increase or decrease in the model whereas a relationship of the negative causal indicates that an increasing or decreasing of the variable A lead to decreasing or increasing of the variable B in the model. The component of system dynamics is shown in Fig. 2 (Boateng *et al*., 2013).

A casual relationship: The (+ -) Signs at the arrowheads refer to the effect is positive (negative) regarding the cause/sign of the arrow refers to material and/or information delay R indicate Reinforcing loop and B the Balancing loop. The researcher made a survey on the programmer ask them about the cause of the viruses and worms and their effect on the computers, the results of the survey as follow in Table 1.

Also, the researchers asked about the best personal computer characteristic which was portege Z30-C-138, comes with Intel Core i7 processor with Intel HD Graphics 520 graphics card, 16GB random access memory, 13.3-inch display with 1920×1080 pixel resolution and 512 GB internal memory SSD with battery that can work up to 11 h continuously. This will later come with benefit to build the model.

Table 1: The results of the survey

Attack/cause	Effects	Percentage
Worms		
Exploite system design Vulnerablities	Network disable	90
Viruses		
Exploited system design Vulnerabilities	Slow the speed	90

RESULTS AND DISCUSSION

The model that built using system dynamic in Vensim program. the first step is to build the model without any attack and simulate the basic operation performed by the computer which are inputs, processing, output and storage as follow. Figure 3 represent the initial model without the effect of any attack.

Algorithm 1; Vensim program:

Start
No of task = 4
Work quality = 0.9
Work To Do = rework discovery rate-work flow
Miss work = work flow*(1-Work Quality)
IF (Work Accomplish/(Work Accomplish Work To do)))< = 0
THEN
Time to detect error = (4/16)
ELSE
Time to detect error = (3/16)
Rework = Miss Work-rework discovery rate
rework discovery rate = Rework/Time to detect an error
IFWorkflow = Work Is Done
THEN
Workflow = 0
ELSE
Work flow = 2
Work Accomplish = workflow
End

Every variable in this model is related to other variable using the equation and this equation is concluded from the observation of the variables

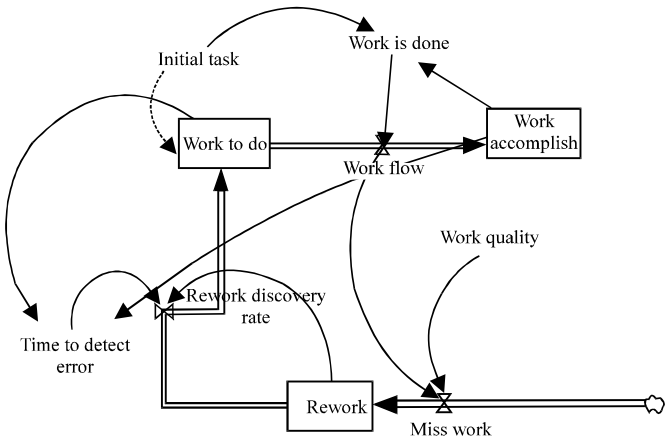

Fig. 3: The simnulation of the four tasks

behaviors. The work to do represent the amount of the tasks required to be done by the computer and its fed by the initial task which is four tasks, the work is done represent the amount of the work required and the quality represent 0.9 which mean that 90% of the work accomplish and 10% required to be reworked, time to detect error is the time required to discover the error, the number 16 relate to the speed of the computer (Fig. 4). This show at the first, we need additional tasks to the rework and then once the computer fix the error the tasks become zero the above is the same as the original model but the effect of viruses and worms are added.

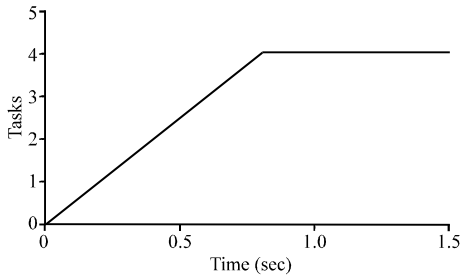

Fig. 4: The simulation of work accomplish

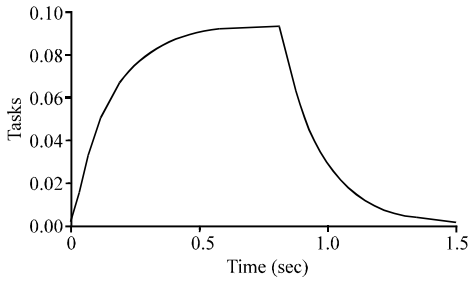

Fig. 5: The simulation of rework

Algorithm 2; Simulation of rework:

Start
Work To Do = performance error generate +rework discovery rate-work flow
IF ((Work Accomplish/(Work Accomplish+Work To Do))< = 0
THEN
Time to disable = (1/16)
ELSE
Time to disable = (2/16)
Performance Error = error generate-performance error generate
End

Figure 5 shows the effect of the viruses and worm as viruses cause speed to be slow and the work cause the network to be disabled and both lead to cause performance error (Fig. 6 and 7). The above show that under the effect of worms and viruses on the tasks performed by the computer will be less as it cause computer disable of the work and also slow the speed of it (Fig. 8).

This show the number of the task that will cause the performance error, at the first iteration with effect only with viruses the number of task is <6, then when they both affect it become more than 6 tasks. Although, the number of original tasks are four the main task divided into subtask to perform the work. The above show that the computer will continually need tasks to rework and never become zero which mean additional effort (Fig. 9 and 10). The above figure show the error generate with effect of both viruses and worms which both lead to at least 6 task.

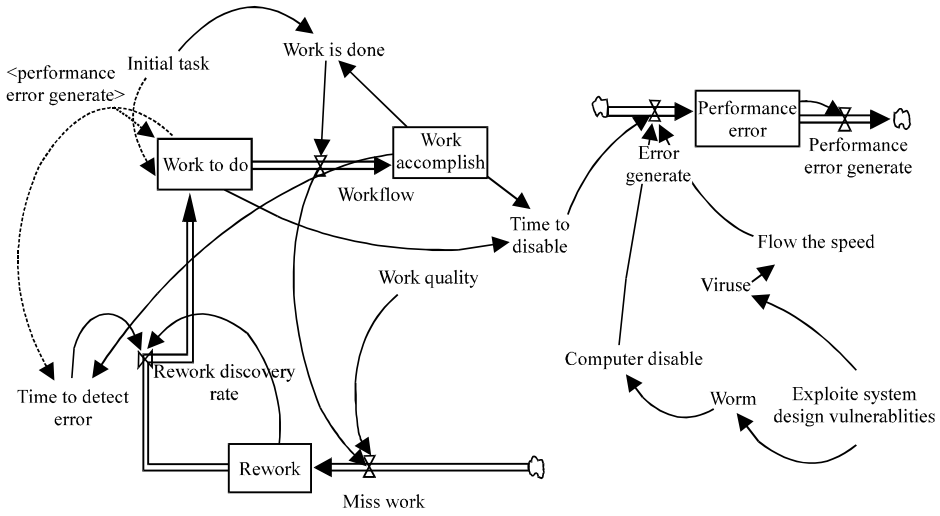

Fig. 6: The simulation of the computer affected by viruses and worms

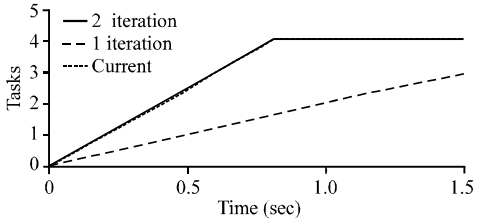

Fig. 7: The simulation of work accomplish effected by viruses and worms

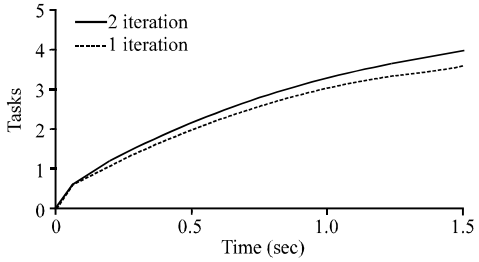

Fig. 8: The simulation of performance error effected by viruses and worms

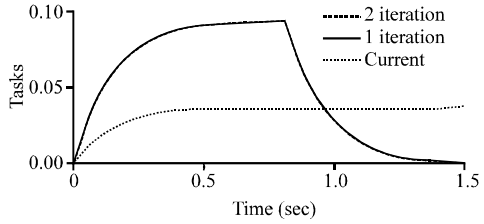

Fig. 9: The simulation of rework effected by viruses and worms

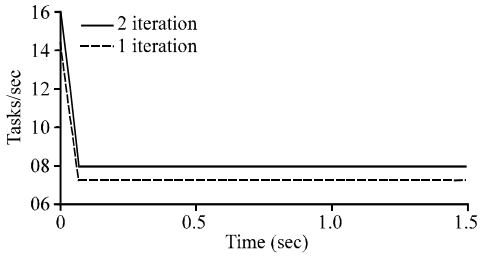

Fig. 10: The simulation of error generated affected by viruses and worms

CONCLUSION

The viruses and worms can cause series defects in the computer and it need to follow their behavior dynamically to notice the changes that occur in the computer in relatively small periods. The effect of the viruses and worm as viruses cause speed to be slow and the work cause the network to be disabled and both lead to cause performance error and thus the effect of worms and viruses on the tasks performed by the computer will be less as it cause computer disable of the work and also, slow the speed of it. Finally, we can conclude that system dynamics is the powerfultool in analyzing the behavior of the worms and viruses in the computers and it should be used to explore more effect of these two attack.

REFERENCES

Barwise, M., 2014. What is an internet worm?. BBC, London, UK.

Boateng, P., Z. Chen, S. Ogunlana and D. Ikediashi, 2013. A system dynamics approach to risks description in megaprojects development. Organiz. Technol. Manag. Constr. Intl. J., 4: 593-603.

Cohen, F.B., 1991. A case for benevolent viruses. Master Thesis, Fred Cohen & Associates, Pittsburgh, Pennsylvania.

Ford, D.N., S.D. Anderson, A.J. Damron, R.D.L. Casas and N. Gokmen *et al*., 2004. Managing constructibility reviews to reduce highway project durations. J. Constr. Eng. Manag., 130: 33-42.

Forrester, J.W., 1961. Industrial Dynamics. MIT Press, Cambridge, Maryland.

Fox, J., 2006. Consumer reports, viruses cost USA $5.2 Billion. Consumers Union, Yonkers, New York, USA.

Li, J. and P. Knickerbocker, 2007. Functional similarities between computer worms and biological pathogens. Elsevier Comput. Security, 26: 338-347.

Li, X., 2003. Computer viruses: The threat today and the expected future. Master Thesis, Department of Electrical Engineering, Linkoping University, Linkoping, Sweden.

Martin, G.J. and J. Sterman, 2017. Theory and Practical Exercises of System Dynamics. 4th Edn., Barcelona Publisher, New Braunfels, Texas, USA., Pages: 282.

Stallings, W. and L. Brown, 2012. Computer Security: Principles and Practice. 2nd Edn., Pearson Education, Upper Saddle River, New Jersey, ISBN: 9780133072631, Pages: 816.

Stallings, W., 2003. Cryptography and Network Security Principles and Practice. 3rd Edn., Prentice-Hall of India Pvt. Ltd., India.

Tang, Y., J. Luo, B. Xiao and G. Wei, 2009. Concept, characteristics and defending mechanism of worms. IEICE Trans. Inf. Syst., E92: 799-809.

Wack, J.P. and L.J. Carnahan, 1989. Computer Viruses and Related Threats: A Management Guide. Diane Publishing, Gaithersburg, Maryland, USA., ISBN-13:9781568068527,.