IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

Computer Virus : Open Problems

Ankur Singh Bist
Govind Ballabh Pant University Of agriculture And Technology, India
ankur1990bist@gmail.com

Abstract

Computer viruses are very typical problem for society and this problem is quite typical to solve . There are various reasons due to which this special problem is not getting solved completely .In this paper we will focus on various open problems regarding the concerned domain .

Keywords: Open problems , Heuristic .

Introduction

Computer viruses have the property of self-replication and they are supposed to have artificial life but their survival and expansion is very harmful since their activity creates threat for issues like privacy . There are following techniques that get used to detect computer viruses .

1. Signature based detection
2. Smart scanning
3. Skeleton detection
4. Heuristic analysis
5. Filtering
6. Generic detection

These methods of computer virus detection are used but they show false positive and false negative rates since there are various open issues in computer virology that prevents to resolve this issue completely . In this paper we will try to focus on some issues from various domains that are responsible for open problems in computer virus research.

Open Issues

1. There are various heuristics that are used to detect the computer viruses the result of using heuristics may be inexact so their is always a doubt the techniques developed using heuristics will behave and how many problems will arise in it [1].

2. The issue of computer virus spread is another factor that includes birth rate , death rate and various pattern between program . These factors need to be analysed because they still produce a kind of mystery[1].

3.There should be digital immune system that must be developed centrally to extract signature and distribute globally[1] .

4. We always defend for computer viruses , there should be a system to develop the system that analyse the future behaviour of computer viruses so that they can be prevented .

Source code fragmented malware has been proven to be NP complete in general .

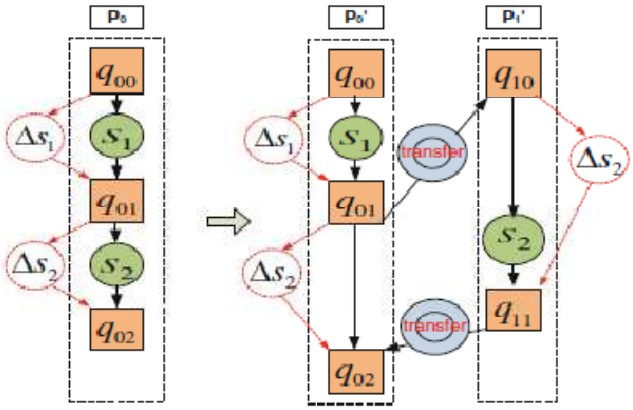

Fig. Shadow attack[2]

Detection of shadow attacks is NP complete[2].

Definition A *shadow attack* can be regarded as a program transformation function SA_p : given a program p and some malware specifications M as inputs, SA_p will generate a multiple-process program p' with two properties: (i) *Detect*(p')*–False* while *Detect*(p)*–True*, (ii) p' has the same functionality as p.

The issue of open problem regarding computer viruses can be seen in mathematical domain . As far as computing is concern Turing machine is an universal tool but there are lot of problems that can not be solved by Turing machine .

Hopcroft and Ullman (1979, p. 148) formally define a (one-tape) Turing machine as a tuple [3]

$M = \langle Q, \Gamma, b, \Sigma, \delta, q_0, F \rangle$ where

- Q is a finite, non-empty set of *states*
- Γ is a finite, non-empty set of the *tape alphabet/symbols*
- $b \in \Gamma$ is the *blank symbol* (the only symbol allowed to occur on the tape infinitely often at any step during the computation)
- $\Sigma \subseteq \Gamma \setminus \{b\}$ is the set of *input symbols*
- $q_0 \in Q$ is the *initial state*
- $F \subseteq Q$ is the set of *final* or *accepting states*.
- $\delta : Q \setminus F \times \Gamma \to Q \times \Gamma \times \{L, R\}$

is a partial function called , where L is left shift, R is right shift. (A relatively uncommon variant allows "no shift", say N, as a third element of the latter set.)According to Church theorem if an algorithm exists it can be solved by Turing machine . It is impossible to create a Turing machine to determine if a given TM will stop or not using specific input .The limitations of Turing machine also come as a barrier to make a complete defensive mathematical model for computer viruses it is due to the fact that viruses have grown upto typical forms like metamorphic viruses that have various variant making capacity , these type of successive growth of computer viruses created a challenge among the researchers involved in computer antivirus design . Fred cohen in proved that the general problem of detecting computer virus is undecidable . D. Spinellis proved that the detection of bounded length polymorphic virus is NP complete . There are various issues related to complexity and classification regarding computer viruses[4].

1. If infected program set is undecidable , what is it's time complexity ?
2. If infected program set , what is the time complexity of recursive set containing infected program set ?
3. It has been proved that polymorphic viruses with infinite form exists but have not seen yet in real world . The open issue in this particular respect is that computability paradigm would produce will produce non trivial polymorphic viruses while considering real program .
4. With respect of polymorphic and metamorphic viruses it can be stated that mutation process classification is an open problem .
5. There are various issues also related to quantum viral detection .
6. There are various conflicting issues related to virus propagation models .
7. It is very typical to determine the malicious behaviour by analysing the malicious codes.
8. There are various issues related to true classification of malicious codes .
9. There are various issues in existing detection techniques regarding false positive and false negative .
10. There are issues related with developing high accuracy compilers to scan malicious codes .

The issues mentioned above are crucial issues for those who want to explore the issue of malicious codes . The other important issue related to open issue can be seen in while we see the problem of computer virus in biological domain actually the intension remains in this to map this towards the solution that can be obtain from biological domain . Nature provides protective measure to each species called the immune system that gives one the capability to defend itself . The foreign elements make attack on the body elements called non self and self respectively .Various essential terms used in immune system:---

1. Antigen---Foreign protein , attacker
2. Antibody---make binding to antigen for their destruction

It is just similar to scenario of computer virus the external element or files contain malicious activities in them like antigen that it is duty of our computer immune system to make detection of that intruder and make removal .It's inspiration can be taken from immune system and a specific activity can be performed as done by antibody for the detection of computer virus and all this is to be done under the framework of artificial immune system.

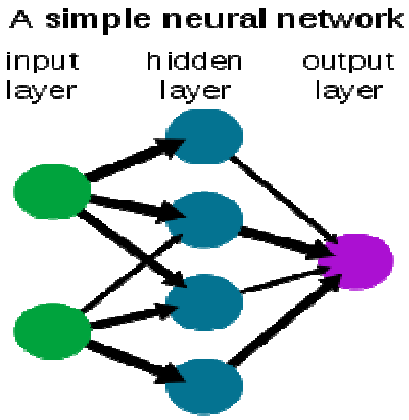

Fig . neural network [3]

Neural networks and genetic algorithms are widely used in this domain but the issue lies while self non-self factor is calculated the artificial immune system designing also includes various challenges that comes under open issue . The way by which proper classification can be made between self and non-self must be traced properly to resolve the open issue in biological domain .

Conclusion

In this paper various issues are discussed that contains open problems of computer virology . Mathematical domain that identifies and works for computer viruses identification is defined with limitations . Biological study of viruses and their mapping with computer viruses with open issues are defined . This study will help to analyse the issue of computer viruses and will be effective in term of develop a defensive approach .

References

[1] Steve R. White ,"Open problem in computer virus research", USA.

[2] Weiqin Ma , Pu. Duan, Sanmia Liu, Guofei Gu ,"Shadow attacks : automatically evading system call behaviour based malware detection " springer .

[3] www.wikipedia.com Eric Filiol ,"Open problem in computer virology " .