IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

Mathematical Approaches For Computer Virus

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

Abstract

This paper presents various aspects of mathematical approaches that are used to make analysis of computer viruses . The theory of functions ,logics and the automata theory helps to understand the replicating behaviour of computer viruses with this methodology leads to various detection strategies .

Keywords :- Recursive ,Replication.

Introduction

Computer viruses are big threat to computer world , researchers doing work in this area have various effort in the direction of classification and detection methods of these viruses . Graph mining , system call arrangement and graphical analysis are some of the latest research activities in this field . The computability theory the semi computable functions, computable functions are quite important in our context of analysing malicious activity .

Mathematical models like random access stored program machine with the association of attached background is used by Ferenc Leitold while explaining modelling of viruses in his paper.

Computer viruses like polymorphic viruses and metamorphic viruses have more efficient techniques for their evolution so it is required to use strong models to understand their evolution and then apply detection followed by the process of removal.

Mathematical Elements

Computability theory is also known as computability theory .In Computability theory a semi computable function means a partial function F:Q→R and these are approximated using above and below side called upper semi computable and lower semi computable .
Hopcroft and Ullman (1979, p. 148) formally define a (one-tape) Turing machine as a tuple [4]
$M = \langle Q, \Gamma, b, \Sigma, \delta, q_0, F \rangle$ 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*.
- $\delta : Q \setminus F \times \Gamma \rightarrow Q \times \Gamma \times \{L, R\}$ 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.)

Mathematical Approaches

Computer viruses are dangerous due to their abnormal behavior also called functions of it to explain their activities mathematically one crucial aspect are functions .

How virus propagate? , The fundamental logics of self replication is there. In mathematics generally one concept that can map to it are the recursive functions .The functions that call to themselves are called recursive functions, one common factor among recursion theory is that ,there should be a terminating condition that could stop recursion , if that condition is not there the function will move infinitely so if we map this scenario with virus scenario we get various factors of similarity .

One factors is the factor of expansion of population of copies of the entities, secondly the factor of controlling that growth as per required condition .

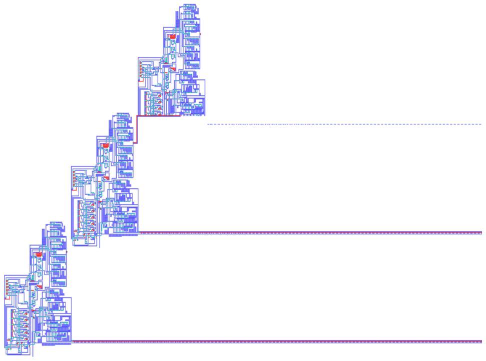
G. Bonfante ,M. Kaczmarek, and J.Y. Marion in their paper of " abstract detection of computer viruses " defined the scenario of virology on the basis of three fundamental functions[2,5] .

1. Enumeration recursive function
2. Semicomputable functions
3. Propagation functions

The synergy of these functions together defines the various growth parameters in very lucid manner.
Any virus spread in the system or network must be identified for their detection so the decidability factors of function becomes crucial for detection of viruses.

Rice theorem states that for any nontrival properties of the partial functions there exists no general and efficient method to identify whether a computation decides partial function with that property and the interrelationship of these functions are necessary for virus detection.

John von Neumann's **Universal Constructor** is a self- replicating machine in a cellular automata (CA) environment.
In 1940 it came into existence without any use of computers. Von Neumann's specification defined the machine as using 29 states, these states constituting means of signal carriage and logical operation, and acting upon signals represented as bit streams[1,4].The organization of entities and supporting units in this architecture leads to provide us a map towards our problem of the self replicating behavior of computer viruses . A 'tape' of cells encodes the sequence of actions to be performed by the machine. Using a writing head (termed a construction arm) the machine can print out (construct) a new pattern of cells, allowing it to make a complete copy of itself, and the tape[1,4].



The first implementation of von Neumann's self-reproducing universal constructor [1,4].

Another aspect to look towards viruses is done by using the logic theory the fundamental of automata theory that provides help to understand the certain problem in various ways is very effective if the parallel processing is done with logic theory .The problem arises with static methods of virus detection is that the number of virus signatures is increasing with rapid manner so only way to detect new born virus signature should be any dynamic method . The dynamic method can be designed by making a semantic analysis of the certain problem so our approach given here can be used to make the identification eaiser.

The backtracking idea of the process of self replication as done by machine would be very much helpful to obtain the idea ,"how to break this phenomena of self replication to save our system or network from attack".

The Turing machines have enormous potential but there are some points where it doesn't work. It is not possible for a Turing machine to determine that on a particular input turing machine will stop or not but when the concept of sequence matching concepts get merged in this domain the we can create a finite boundary for detection of viruses.

The evolution of computer viruses from simpler encrypted viruses now have made a journey passing through polymorphic viruses , oligomorphic viruses ,metamorphic viruses , computer worms and botnets . The rate of infection and the process used by virus designers are increasing day by day . What is needed from the side of security provider to map all the worst situations created by virus designers , the core problem we signify running in all the themes that are used to sort out the problems of computer viruses in this case the fundamental mathematical model creation is giving a new direction to the problems arising in this field. Firstly defining the viruses based on the certain mathematical bases as described in this paper and then make a simulation scenario that can be very much helpful to analyze the concerned problem[3,5] .

Conclusion

In this paper we make a look on various approaches to analyze the virology in the domain of functions and turing machines with other entities . This observational study is quite supporting in terms of defining , classifying and detecting certain types of computer viruses. The further analysis and implementation of all facts and concepts will surely lead to the formation of more stronger detection and analysis of computer viruses. Another mathematical model includes the various probability based process one of the most popular is hidden markov model that is widely used in this domain its variant profile hidden markov model also get used . Various classifiers that works on layering approaches uses the probability applying approaches. So It is required to apply the proper and collective methodology from all these entities so that it could be easy to gain the hidden synergy of these process.

References

[1] Pesavento, Umberto (1995), "An implementation of von Neumann's self-reproducing machine".

[2] G .Bonfante ,M. Kaczmarek ,and J.Y. Marion , “Abstract detection of computer viruses .”

[3] Ferenc Leitold , “Mathematical model of computer viruses” Veszperm University ,Hungary.

[4] Davis ,M. , Computability and unsolvability, McGraw-Hill,New York.