IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

Fuzzy Logic for Computer Virus Detection

Ankur Singh Bist
Quantum Global Campus, Roorkee, India
ankur1990bist@gmail.com

Abstract

Computer viruses are big threat to computer world; researchers doing work in this area have made various efforts in the direction of classification and detection methods of these viruses. Graph mining, system call arrangement and CFG analysis are some latest research activities in this field. The computability theory and the semi computable functions are quite important in our context of analyzing malicious activities. A mathematical model like random access stored program machine with the association of attached background is used by Ferenc Leitold while explaining modeling of viruses in his paper. Computer viruses like polymorphic viruses and metamorphic viruses use more efficient techniques for their evolution so it is required to use strong models for understanding their evolution and then apply detection followed by the process of removal. Code Emulation is one of the strongest ways to analyze computer viruses but the anti-emulation activities made by virus designers are also active. This paper involves the fuzzy logic techniques used for detection of computer viruses in better manner.

Keywords: Fuzzy Logic, Malicious Codes.

Introduction

Computer viruses are various processes that have been used in the direction of classification of computer virus from normal files that will finally lead to computer virus detection. Machine learning techniques are widely used in this direction. As statistics says that the attacks of malicious codes are increasing day by day so there is requirement of strong techniques that can be used for their detection. Computer virus designers use lot of techniques that are difficult to analyse and detect. The static methods also seems not to work in the case where every time there are rapid dynamicity from attacker side so now a days main focus is going towards the methods that are dynamic and are able to detect zero day computer virus.

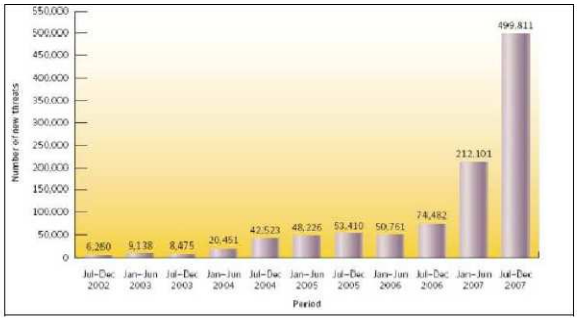
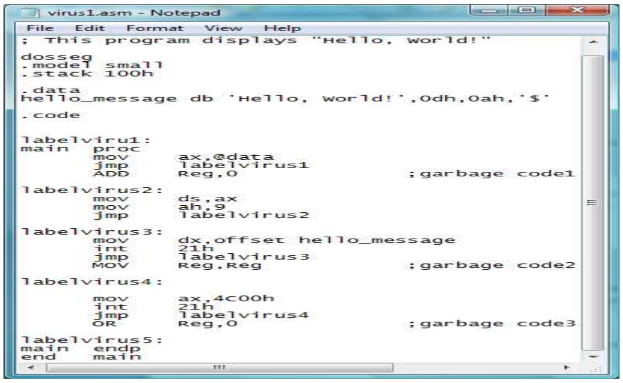


Figure1 Malicious threat rise [1]

The rise in the malicious threats like computer virus activities are required to be handled and observed strongly to make certain defence that can stand as a saviour of security domain. Other types of malware are:

1. Viruses
2. Trojan horse
3. Botnets
4. Adware
5. Spyware



```
; This program displays "Hello, world!"

dosseg
.model small
.stack 100h

.data
hello_message db 'Hello, world!',0dh,0ah,'$'

.code

labelviru1:
main    proc
        mov     ax,@data
        jmp     labelvirus1
        ADD     Reg,0                   ;garbage code1

labelvirus2:
        mov     ds,ax
        mov     ah,9
        jmp     labelvirus2

labelvirus3:
        mov     dx,offset hello_message
        int     21h
        jmp     labelvirus3
        MOV     Reg,Reg                 ;garbage code2
labelvirus4:

        mov     ax,4C00h
        int     21h
        jmp     labelvirus4
        OR      Reg,0                   ;garbage code3

labelvirus5:
main    endp
end     main
```

Figure2. Assembly file for virus code [2]

The mutating behaviour of metamorphic viruses is due to their adoption of code obfuscation techniques.

a) Dead code insertion
b) Variable Renaming
c) Break and join transformation
d) Expression reshaping
e) Statement reordering

ISSN: 2277-9655
Impact Factor: 1.852

Fuzzy Logic

Fuzzy logic is a form of many-valued logic; it deals with reasoning that is approximate rather than fixed and exact. Compared to traditional binary sets (where variables may take on true or false values) fuzzy logic variables may have a truth value that ranges in degree between 0 and 1. Fuzzy logic has been extended to handle the concept of partial truth, where the truth value may range between completely true and completely false. Furthermore, when linguistic variables are used, these degrees may be managed by specific functions. Irrationality can be described in terms of what is known as the fuzzjective.

With the 1965 proposal of fuzzy set theory by Lotfi A. Zadeh, the fuzzy logic was come into existence. Fuzzy logic has been applied to many fields, from control theory to artificial intelligence.

Classical logic only permits propositions having a value of truth or falsity. The notion of whether 3+3=6 is absolute, immutable, mathematical truth. However, there exist certain propositions with variable answers, such as asking various people to identify a color. The notion of truth doesn't fall by the wayside, but rather a means of representing and reasoning over partial knowledge is afforded, by aggregating all possible outcomes into a dimensional spectrum.

Both degrees of truth and probabilities range between 0 and 1 and hence may seem similar at first. For example, let a 200 ml glass contain 60 ml of water. Then we may consider two concepts: Empty and Full. The meaning of each of them can be represented by a certain fuzzy set. Then one might define the glass as being 0.7 empty and 0.3 full. Note that the concept of emptiness would be subjective and thus would depend on the observer or designer. Another designer might equally well design a set membership function where the glass would be considered full for all values down to 100 ml. It is essential to realize that fuzzy logic uses truth degrees as a mathematical model of the vagueness phenomenon while probability is a mathematical model of ignorance.

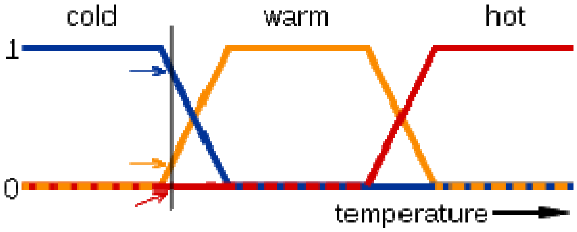


Figure 3. Function mapping on temperature scale

In this image, the meanings of the expressions *cold*, *warm*, and *hot* are represented by functions mapping a temperature scale. A point on that scale has three "truth values"—one for each of the three functions. The vertical line in the image represents a particular temperature that the three arrows (truth values) gauge. Since the red arrow points to zero, this temperature may be interpreted as "not hot". The orange arrow (pointing at 0.2) may describe it as "slightly warm" and the blue arrow (pointing at 0.8) "fairly cold.

An e-epidemic SIRS (susceptible–infectious–recovered–susceptible) model for the fuzzy transmission of computer virus in computer network is formulated by authors. They analyzed the comparison between classical basic reproduction number and fuzzy basic reproduction number, that is, when both coincide and when both differ. The three cases of epidemic control strategies of computer virus in the computer network–low, medium, and, high–are analyzed, which may help us to understand the attacking behavior and also may lead to control of computer virus. Numerical methods are employed to solve and simulate the system of equations that defines different states required for study.

Organizations and individuals today need to have a comprehensive virus protection policy to face the growing threats of the Internet computer viruses. Given the rise in micro viruses within the last three years many organizations have adopted a proactive management approach to the problem by installing antivirus and content filtering software in order to identify and prevent computer viruses threats. Due to availability of much antivirus and content filtering software, their evaluation and selection requires a multiple criteria decision-making method. Authors applied the analytic hierarchy process (AHP), a well-known multiple criteria decision making method, which is designed for decisions that require integration of quantitative and qualitative data, to evaluate and select antivirus and content filtering software. Role of fuzzy techniques and methods will be helpful for these kinds of studies in future and to fight with zero day virus attacks. Fuzzy methods with other techniques in hybrid forms are being used to mitigate and resolve the issue of computer virus threat.

Conclusion

This paper discusses about basic outline of computer viruses and their detection using fuzzy logic. The methods discussed are being used for solving different problems. The impact of fuzzy technique in the direction of computer virus detection is mentioned. This study will be helpful for researchers working in the field of computer virology.

References

[1] www.wikipedia.com.
[2] Christian Wressnegger, ”Beatrix: A Malicious CodeAnalysis Framework”.

ISSN: 2277-9655
Impact Factor: 1.852

[3] S. Papadimtrou and J. Sun. Disco: distributed co clustering with map reduce. In proceedings of ICDM, 2008.

[4] BitShred: feature hashing malware for scalable triage and semantic analysi

[5] Bimal Kumar Mishra, Samir Kumar Pandey, Fuzzy epidemic model for the transmission of computer viruss in computer network.

[6] Farrokh Mamaghani , Evaluation and selection of an antivirus and content filtering software Department of Management, St John Fisher College, Rochester, New York, USA)