SPECIMEN FORMAT FOR THESES OF MONTH

Faculty	:	Science
Department	:	Computer Science
Branch/ Area:	:	Computer Science
Sub Subject Heading:	:	Network Security
Candidate's Name	:	S.Divya
Candidate's Address with email	:	10.S.S.Nagar, First Street, Kongu Main Road, TNK Puram, Tirupur-641607
Title of the thesis	:	Characteristics based Detection of Internet Worms using Combined Machine Learning Methods and Worm Containment
(i) In Roman Script (ii) In roman Script		-
Nomenclature of Degree:	:	Ph.D
Month & Year of Enrolment:	:	July 2012
Month & Year of Registration:	:	July 2012
Month &Year of Submission:	:	June 2015
Month &Year of Award	:	February 2016
Name of Supervisor	:	Dr.G.Padmavathi
Designation of Supervisor	:	Professor and Head of Department
Centre/department/school in which research was conducted	:	Computer Science, Avinashilingam Institute for Home Science and Higher Education for Women
University's Name & Address	:	Avinashilingam Institute for Home Science and Higher Education for Women, University Coimbatore – 641 043.

Abstract within 300 words:

With the rapid growth of Internet today, many Internet based applications are evolving. Internet is an open network accessed by all. The major challenge in Internet is security. Many attacks and vulnerabilities affect the network. Among the various attacks, Internet worms are vulnerable because they infect a large number of hosts within a short period of time and from that infected hosts they further initiate attacks like distributed denial-of-service, phishing and spyware through their propagation. Internet worms like "Code-Red" in 2001, "Slammer" in 2003, "Witty"/ "Sasser" in 2004, Storm in 2007, Conficker in 2008 and StuxNet in 2010-2012 have created prominent damages to the hosts. Within the period of five years, 4,00,000 computers got infected due to Blaster worm in 2003. Conficker worm damaged approximately 13 million IP addresses. This number may increase year by year. To overcome these damages and to defend against these attacks, effective defense mechanism is necessary. Therefore, detection and containment of Internet worms are the need of the day. For Internet Worm detection, there are two main approaches existing namely, signature based and anomaly based. Out of the two, anomaly based detection schemes provide better detection on newly appearing worms. There are various anomaly based detection approaches exist in the literature such as Probabilistic modeling, Spectrum based, Statistical estimation, Game theory, Epidemic spreading and Machine learning methods. Among these approaches, Machine Learning methods provide faster detection accuracy for rapidly changing Internet worms. Containment methods are applied to prevent the network from further infection after detection.

Based on the challenges created by Internet worms, the objectives of this research work are formulated after studying significant literatures. Though Internet worms are detected using different Machine Learning Approaches, the detection based on the characteristics of worms provides for better detection of new unknown worms. The characteristics refer to the nature of worms and it makes the detection effective at the initial stages of the propagation itself.

A Three-Step Methodology is proposed with four contributions to meet the objectives of the thesis. The Internet worm detection is done using the combined Machine Learning Methods based on anomaly detection schemes and Containment based on blocking schemes. The proposed **P**rincipal Component Analysis with **M**ulticlass Support Vector Machine and **R**abin Footprint Algorithm ***(PMR)*** detects the Malcode existence in the downloaded programs based on unknown signatures. The detected and classified Malcode programs are contained to prevent from further infection. The proposed **D**eterministic Finite Automata with **F**uzzy Logic Classifier and **F**ilter-Ary Sketch ***(DFF)*** performs detection and containment of malicious contents in packets based on payload. The proposed **E**nhanced **C** 4.5 Algorithm and **B**lacklist ***(ECB)*** detects and contains the unused addresses based on illegal traffic. The proposed **k**ernelized **E**xtreme Learning Machine with **A**utomated Worm Containment Algorithm ***(kEA)*** is used for detection and containment of malicious traffic from non-existing IP addresses based on connection attempt failures.

The proposed methods are implemented using Java NetBeans IDE 7.4 and Microsoft SQL Server. The parameters used for evaluation are Memory Utilization, Time Consumption, Precision Value, Recall Value, Accuracy, Detection Rate and Containment Rate. In contribution one, the detection accuracy achieved by the proposed ***PMSVM*** is improved by 13.57% and all the detected Malcode programs are blocked using ***PMR*** with 100% containment rate. The time taken to contain the detected programs is 200ms. In contribution two, the proposed ***DDF*** method achieved better detection accuracy with improved 0.23% and proposed ***DFF*** method achieved containment rate with 100% and

the time consumed to block is 1300ms. In contribution three, the proposed ***CPC*** method for detection of illegal traffic achieved detection accuracy improved by 14.47%, and proposed ***ECB*** method provides containment with 100% of blocking all detected malicious traffic within 20 ms. In contribution four, the proposed ***kELM*** method achieved detection accuracy improved by 23.67%. Finally, the proposed ***kEA*** method blocks all the detected malicious IP addresses with 100% containment at the time span of 33ms. The four contributions based on combined Machine Learning Methods provide better detection and containment of newly appearing Internet worms entering the networks.

The proposed research methodology can be applied for other characteristics of Internet worms like hitlist, topological and web search target finding worms with polymorphic and metamorphic payload schemes. The proposed methodology can be integrated with the hardware devices at the Network Intrusion Detection System to handle real attacks affecting the network.

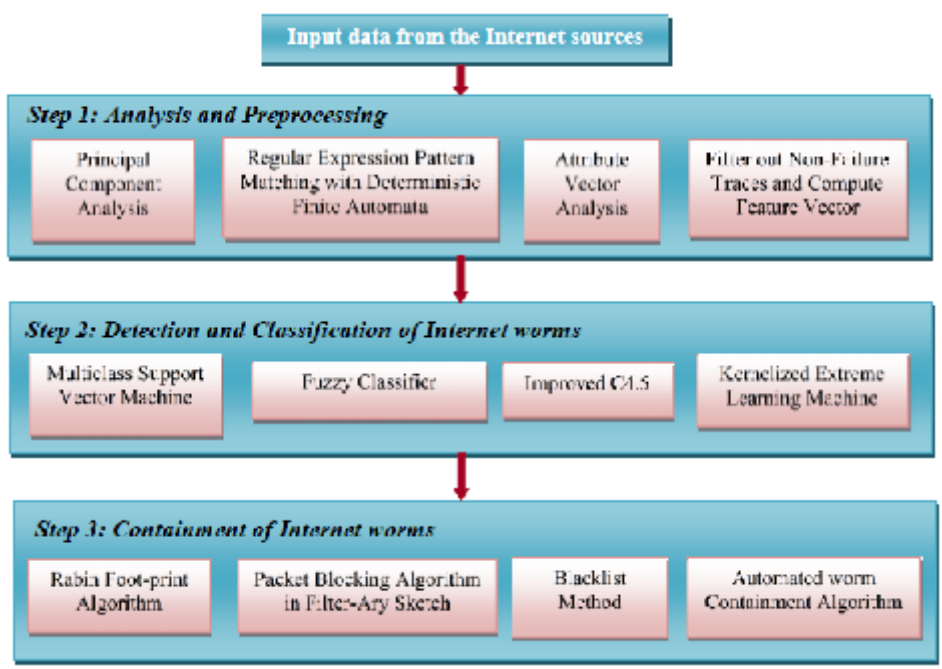
i) Major objectives :

The objective of the research work is to device a defense mechanism achieving better detection and containment of Internet worms.

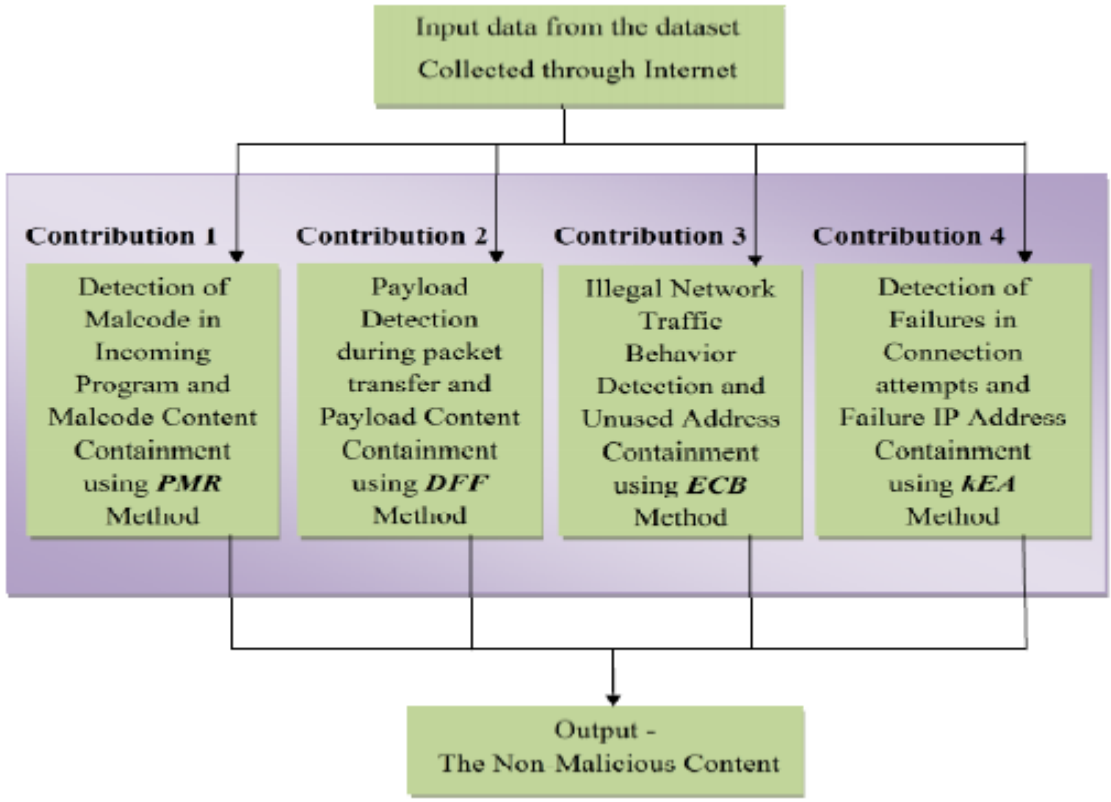
The secondary objectives of the thesis are:

- Improve the detection and classification accuracy
- Reduce the memory utilization
- Minimize time consumption
- Increase precision value
- Maximize recall value
- Enhance containment rate

ii) Methodology :



iii) Findings:



Examiners

Internal Examiner : Dr.Manjaiah .D.H
Professor,
Department of Computer Science,
Mangalagangotri,
Mangalore University,
Mangalore:574 199,
India.

External Examiner : Dr.S.Arockiasamy
Head of the Department
Department of Information Systems
University of Nizwa
PC:33, P.O.Box:616, Birkat Al Mouz,
Nizwa, Sultanate of Oman.