CHARACTERISTICS BASED DETECTION OF INTERNET WORMS USING COMBINED MACHINE LEARNING METHODS AND WORM CONTAINMENT

CHAPTER 8
CONCLUSION AND FUTURE DIRECTIONS

8.1. Summary and Conclusions

8.2. Future Research Directions

In this recent world of Internet, it is important to secure the data from the security threats like worm attack. During the past 20 years, Internet worms have caused serious infection on the network and heavy financial losses worldwide. Internet worms are creating dangerous threats in the network thereby compromising communication security. The goal of this research work is to provide better defense mechanisms against Internet worms.

This chapter discusses the conclusion of this research work. The future direction for this research work is also stated in this chapter.

8.1. Summary and Conclusions

The chapter describes the discussed contents in the previous chapters and provides the summary of the thesis. In order to achieve the goal of this research work, a three-step methodology is proposed and techniques are applied. Four contributions proposed in this thesis give better detection accuracy and containment of detected Internet worms.

Based on the literature study, it is observed that the existing methods require few improvements for better detection and containment of Internet worms. Combined Machine Learning Methods under Anomaly based detection approaches are used in this research work to improve the detection accuracy. Based on the characteristics of Internet worms, the defense schemes have been applied to defend against Internet worms effectively.

The proposed ***PMR Method*** is introduced to detect and block the unknown malcodes existing in the programs. The programs that are downloaded in the host with malicious codes are detected and classified based on unknown signatures. Then, they are blocked to prevent the host from further infection.

The proposed ***DFF Method*** provides better detection and containment of packet payloads. The exploitation done by payloads through vulnerable applications are detected using pattern matching and are classified as malicious. The hashed malicious payloads are blocked for preventing transfer of payloads in the network.

The proposed ***ECB Method*** is used to detect and block the unused IP addresses based on illegal traffic. The traffic from unused addresses are analyzed using the attribute

vectors and classified. The detected malicious IP addresses are blocked to prevent further illegal traffic propagation in the network.

The proposed ***kEA Method*** is introduced to detect and block the malicious traffic created by the worms based on failures in network connections. The failures are detected when the traffic is found from closed target ports or from non-existing IP addresses. Then the failures detected are classified and blocked to prevent the hosts from further infection.

The proposed methods are implemented using Java NetBeans IDE 7.1 and Microsoft SQL Server. The execution of the proposed methods are evaluated using the parameters such as Memory Utilization, Time Consumption, Precision value, Recall value, Detection Rate and Containment Rate. The experimental results show that the proposed methods provide better detection compared to that of the existing methods.

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. The proposed ***DDF*** method achieved better detection accuracy with improved 0.23%, containment rate with 100% and the time consumed to block is 1300ms. Proposed ***CPC*** method for detection of illegal traffic achieved detection accuracy improved by 14.47%, containment with 100% of blocking all detected malicious traffic within 20 ms. Finally, ***kEA*** method achieved detection accuracy improved by 23.67%. Then all the detected anomalous traffic traces are blocked with 100% containment at the time span of 33ms.

The combined four contributions provide better detection and containment of newly appearing Internet worms entering the networks.

9.2. Future Research Directions

This research work is proposed to detect unknown Internet worms based on their characteristics. Only the characteristics like blind scan target discovering, self-carried, second channel and botnet propagating, TCP/UDP transmission and Monomorphic payload format worms are discussed in this research work.

For future work, better detection can be done using the enhanced methods for some more characteristics of Internet worms like:

- In target discovering - Hit list, Topological and Web Server worms
- In Payload Scheme - Polymorphic and Metamorphic worms

The proposed methodology can be integrated with the hardware devices at the Network Intrusion Detection System to handle real attacks affecting the network.