IMPROVING THE DISCRIMINATION ACCURACY RATE OF FLASH EVENTS AND DDOS ATTACKS

SAHAREESH AGHA
02-241172-002

A THESIS SUBMITTED IN FULFILLMENT OF THE REQUIREMENTS FOR THE AWARD OF THE DEGREE OF MASTER OF SCIENCE (SOFTWARE ENGINEERING)

DEPARTMENT OF SOFTWARE ENGINEERING

BAHRIA UNIVERSITY ISLAMABAD

JUNE 2020

Author's Declaration

I, Sahareesh Agha hereby state that my MS thesis titled "Improving the discrimination Accuracy Rate of DDoS Attacks and Flash Events." is my own work and has not been submitted previously by me for taking any degree from this university Bahria University Karachi or anywhere else in the country/world. At any time if my statement is found to be incorrect even after my graduation, the University has the right to withdraw/cancel my MS degree.

Name of scholar: Sahareesh Agha

Date: 22-June-2020

ACKNOWLEDGEMENT

In preparing this thesis, I was in contact with many people, researchers, academicians, and practitioners. They have contributed towards my understanding and thoughts. In particular, I wish to express my sincere appreciation to my main thesis supervisor, Dr. Osama Rehman, for encouragement, guidance, critics and friendship. I am also very thankful to Bahria University and Software engineering department. Without their continued support and interest, this thesis would not have been the same as presented here. Last but not least I would like to thanks to my family and friends for their constant source of inspiration.

ABSTRACT

In our modern age of technologies, Distributed Denial of Service (DDoS) attacks are the most common type of cyber-attacks in communication networks. This is due to the availability of open source and freeware tools. The purpose of the DDoS attacks is to cause interruptions in services availability provided by different network systems, such as web servers. This in-turn results into legitimate users not being able to access the servers and hence facing denial of services. On other hand, flash events are high amount of legitimate requests over a server that occur at specific time periods in result of large number of users visiting a website due to a specific event. As a result, huge amount of network traffic arrived on their servers. Flash events are common network phenomenon which usually occur whenever new/discounted products are launched on companies' site or when an important news is announced. To deal with Flash events, websites use load balancers. However, when DDoS attacks are combined with flash events, they can cause noticeable harm due to the superimposed load on web servers. Hence, it is considered as the best time for attackers to launch a DDoS attack is during flash events. On top of that, DDoS attacks are known to have similar properties to those of normal server requests by mimicking legitimate user traffic, including flash events. As a result, many DDoS packets are failed to be detected by the deployed security mechanisms. Therefore, security mechanism should be intelligent enough to discriminate between DDoS attacks and flash events as its a challenging issue. The purpose of this study is to build an intelligent network traffic classification model to improve the discrimination accuracy rate of DDoS attack from flash events traffic. . Weka is adopted as the platform for evaluating the performance of random forest algorithm.

Experiments executed involve evaluating performance of classifier on 41 attributes present in NSL KDD dataset and with 6 most significant attributes (with

threshold of ≥ 0.5) selected using feature selection technique symmetric uncertainty. To get more confidence on selected attributes (and on threshold value), 3 more experiments are performed, one with 5 most significant attributes, other with 7 most significant attributes and last one without 6 most significant attributes (i.e. the remaining 35 attributes). Experiment results show that Random forest is providing good accuracy of 97.6 with 6 attributes and significant reduction in false positives, false negatives and testing time is observed. Whereas decision tree performance decreases when number of attributes are reduced.

TABLE OF CONTENTS