Network Intrusion Detection for Denial of Service Attacks Using Iterative Algorithms

A Thesis Submitted in Partial Fulfillment of the Requirements for the Master Degree in Information Technology

Submitted by
Faiz Iqbal Tariq Hayat
ID Number: 20055339

Supervised by
Dr. Salman A. Khan
(Assistant Professor)
University of Bahrain

Kingdom of Bahrain
June 2017
Abstract

In today’s age, security has become a fundamental issue in proper and efficient functioning of computer and network systems. This has instigated tremendous research in different sub-domains of network security. One core issue in network security is efficient and timely detection of intrusion such that an attack can be mitigated. Considerable attention has been given to development of efficient intrusion detection systems, both in terms of software and hardware. Among many other approaches, iterative heuristics have been consistently used for network intrusion detection. This study explores the network intrusion detection of Denial of Service Attacks using iterative algorithms. The study documents the occurrences of the different DoS attacks in a typical connection population. Considering this approach, four iterative heuristics, such as the Genetic Algorithm (GA), Cuckoo Search Algorithm (CS), Tabu Search Algorithm (TS), and the Hybrid Cuckoo-Tabu Algorithm (HCTA) have been adapted for DoS intrusion detection in this study. The study also performs a comparative analysis of the aforesaid algorithms in terms of their efficiency in misuse detection on DoS. The proposed algorithms are tested on the benchmark suite of KDD99 dataset. Experiments are done in two directions. The first direction analyzes the performance of the adapted GA for individual attack types. The second direction compares the said algorithms for overall attack detection rate. The results indicate that the adapted GA offers a significant quality of solution. TS, however, outperforms GA, while CS outperforms both GA and TS in terms of DoS attack detection rate. Finally, the study confirms that the HCTA produces the best results among the different algorithms applied in terms of DoS attack detection.