Ain Shams University
Faculty of Science
Department of Mathematics

On Detecting Network Intrusion Using Computational Intelligence

A thesis

Submitted to the Department of Mathematics, Faculty of Science, Ain Shams University, Cairo, Egypt.

For the Degree of M.Sc. In Science as a Partial Fulfillment For Requirements of the Master Science

(Computer Science)

By

Ahmed Abd El-Rahman Mahmoud Elngar

Demonstrator, Faculty of Information Technology & Computer Science, Sinai University, El-Arish, Egypt.

Supervisors

Prof. Fayed Fayek Mohamed Ghaleb
Prof.Emeritus of Mathematics
Faculty of Science
Ain Shams University

Dr.Dowlat Abd El Aziz Mohamed
Lecturer of Mathematics and Computer Science
Faculty of Science
Ain Shams University

List of Publications

Journal Papers:

1. **Ahmed A. Elngar**, Dowlat A. El A. Mohamed , Fayed F. M. Ghaleb, ”A Fast Accurate Network Intrusion Detection System”, International Journal of Computer Science and Information Security, vol. 10, no. 9, pp. 29 - 35, 2012.

2. **Ahmed A. Elngar**, Dowlat A. El A. Mohamed , Fayed F. M. Ghaleb, ”A Real-Time Anomaly Network Intrusion Detection System with High Accuracy”, Information Sciences Letters International Journal, vol. 02, no. 2, pp. 49-56, 2013.

Peer Reviewed International Conference:

1. **Ahmed A. Elngar**, Dowlat A. El A. Mohamed , Fayed F. M. Ghaleb, ”A Real-Time Network Intrusion Detection System with High Accuracy”, The 6th International Conference on Mathematics, Trends and Development (ICMTD12) , 27 - 29 December, Cairo, Egypt, 2012.

Abstract

According to rapid development and popularity of Internet and online procedures, the potential of network attacks has increased substantially in recent years. Therefore, network security needs to be concerned to provide secure information channels. Intrusion Detection System (IDS) becomes an essential component of computer security . Network Intrusion Detection Systems (NIDS) aims to dynamically identify unusual access or attacks to secure the internal networks, by looking for potential malicious activities in network traffic. However, building a high-performance and fast NIDS is a major research problem in network security.

One of the important problems for NIDS is dealing with data containing high number of features. High dimensional data may leads to decrease the predictive accuracy and the speed of the NIDS. Therefore, Feature Selection (FS) is one of the key topics in building NIDS. (FS) can serve as a pre-processing tool for high dimensional data before solving the classification problems. The purpose of the feature selection is to reduce the number of irrelevant and redundant features. (FS) searches for a subset of features which improve the prediction accuracy and improves the NIDS speed.

This thesis is devoted to focuss on how to construct a fast accurate NIDS. The thesis propose two different hybrid NIDS, the proposed hybrid NIDS models involves data preprocessing, data reduction and intrusion classifica-

tion. Experiments and Analysis of the proposed hybrid NIDSs with other previous NIDSs demonstrated that; the two proposed hybrid NIDSs enhance the intrusion detection rate and decreasing the testing speed.

To

My wife Dr. Heba Eid, you supported me each step of my way. You have always been the first to back and strengthen me whenever I felt exhausted and weak.

My baby girl Farida, the smile on your face brings a smile to my heart.

Acknowledgement

*Firstly, **I** would like to thank **ALLAH** for all his grace, mercy and strength that has sustained me throughout this time of my life.*

***I** would like to express my deep thanks and gratitude to **Prof. Fayed M. Ghaleb** for his continuous support, valuable advices and abundant experience throughout this work. **I** have learnt many things about research working from him.*

*I'm indebted to **Dr.Dowlat Abd El Aziz** for her encouragement and helpful co-operation throughout this work. She has provided a lot of motivation.*

*And **I** do not forget to thanks all my teachers, Department of Mathematics Faculty of Science Al-Azhar University ,Ain Shams University and Sinai University on the continued support and encouragement.*

*Finally, **I** would also like to express special thanks to **my father, my mother, my brother, and my sisters** for their love and support during of this work.*

Contents

List of Tables

List of Figures