VARIATIONAL BAYESIAN HIDDEN MARKOV MODEL FOR THE PREDICTION OF DISTRIBUTED DENIAL OF SERVICE ATTACKS

By

AFOLORUNSO, ADENRELE ABOLANLE

Matriculation Number: 029074001

B.Sc. Computer Science and Mathematics (1995), Olabisi Onabanjo University

M.Sc. Computer Science (2004), University of Lagos

A thesis submitted to the School of Postgraduate Studies, University of Lagos, Akoka, Lagos, Nigeria, in partial fulfilment of the requirement for the award of the degree of Doctor of Philosophy (Ph.D.) in Computer Science.

JULY, 2017

AUTHOR'S STATEMENT

I hereby agree to give the University of Lagos Library, a non-exclusive, worldwide right to reproduce and distribute my thesis and abstract (hereinafter "the Work") in whole or in part, by any and all media of distribution, in its present form or style or in any form or style as it may be translated for the purpose of future preservation and accessibility provided that such translation does not change its content.

By the grant of non-exclusive rights to University of Lagos through the Library under this agreement, I understand that the rights of the University of Lagos are royalty free and that I am free to publish the Work in its present version or future versions elsewhere.

Warranties

I further agree as follows:

i. That I am the author of the Work and I hereby give the University of Lagos the right to make available the Work in the way described above after a three (3) year period of the award of my doctorate degree in compliance with the regulation established by the University of Lagos Senate.

ii. That the Work does not contain confidential information which should not be divulged to any third party without written consent.

iii. That I have exercised reasonable care to ensure that the Work is original and it does not to the best of my knowledge breach any Nigerian law or infringe any third party's copyright or other Intellectual Property Right.

iv. That to the extent that the Work contains material for which I do not hold copyright, I represent that I have obtained the unrestricted permission of the copyright holder to grant this license to the University of Lagos Library and that such third party material is clearly identified and acknowledged in the Work.

v. In the event of a subsequent dispute over the copyrights to material contained in the Work, I agree to indemnify and hold harmless the University of Lagos and all of its officers, employees and agents for any uses of the material authorised by this agreement.

vi. That the University of Lagos has no obligation whatsoever to take legal action on my behalf as the Depositor, in the event of breach of intellectual property rights, or any other right, in the material deposited.

_____	_____	_____
Author's Name	Signature/Date	Email
_____	_____	_____
Supervisor's Name	Signature/Date	Email
_____	_____	_____
Supervisor's Name	Signature/Date	Email
_____	_____	_____
Supervisor's Name	Signature/Date	Email

CERTIFICATION

School of Postgraduate Studies, University of Lagos.

This is to certify that the thesis entitled

VARIATIONAL BAYESIAN HIDDEN MARKOV MODEL FOR THE PREDICTION OF DISTRIBUTED DENIAL OF SERVICE ATTACK

Submitted to the School of Postgraduate Studies, University of Lagos for the award of the degree of Doctor of Philosophy (Ph.D.) in Computer Science is a record of original research carried out by:

AFOLORUNSO ADENRELE ABOLANLE

in the Department of Computer Sciences

Author's Name	Signature	Date
First Supervisor's Name	Signature	Date
Second Supervisor's Name	Signature	Date
Third Supervisor's Name	Signature	Date
Internal Examiner's Name	Signature	Date
First External Examiner's Name	Signature	Date
Second External Examiner's Name	Signature	Date

DEDICATION

This thesis is, on one hand, dedicated to the evergreen memories of my parents, Alhaji Alli Folorunso Musari (a.k.a. Agbomola) and Mrs. Sarat Anike Adesola Musari (a.k.a. Iye-Sikira), who together laid a good and solid foundation for this achievement; may Almighty Allah grant them Aljanah Fridaous; and on the other to the selfless and awesome angels that we came from the same loin and sucked the same breasts in persons of Mrs. Serifat Adebukunola Alebiosu, Alhaja Sidikat Olasunkanmi Adesanya, Mrs. Taibat Ibiyemi Yusuf, Mrs. Silifat Olayemi Oyelana, Alhaji Muritala Adekoya Alli (a.k.a. Royal Father), Mr. Azeez Obafemi Afolorunso and lastly, but in no way the least, Mrs. Olufunmilola Olaleye Oyesola, who are forever there to support and buy into every of my dreams, no matter how whimsical.

ACKNOWLEDGEMENTS

All thanks to the Almighty and Ever-living God, the Omnipotent and the Omniscience, for His gift of life, sound health and the resources, both human and otherwise, to embark upon and excel in this academic pursuit. To Him be the glory forever and ever.

Sometimes words and language vocabulary, especially that of a second language, are inadequate to express one's gratitude and appreciation of kind gestures and laudable acts. But, then, express it, we must. This is one of such times. I had the rare opportunity and privilege to be under the tutelage of two great giants in persons of Emeritus Professor Olayide Abass and Professor Harrison O. D. Longe (a.k.a. HOD Natural), who were not only my supervisors, teachers, role models but also my fathers in every sense of the word and mentors par excellence. I appreciate you and say a big thank you not only for allowing me tap into your wealth of academic knowledge and emotional intelligence but also for "adopting" me and accommodating my excesses.

My profound gratitude also goes to my other supervisor, Dr. A. P. Adewole. An extremely humble, kind, dutiful, unassuming and brilliant scholar who is always ready to share his knowledge and guide in a brotherly manner. I thank you sir.

The efforts of Professor Charles Uwadia - a mentor and a father figure – is equally appreciated. His encouragement, support and ideas on my work were unquantifiable and greatly acknowledged. I also acknowledge the support and mentorship of Prof. J. O. A. Ayeni.

Worthy of mention is the various contributions of all the Departmental academic staff towards the successful completion of this programme. My unalloyed gratitude goes to: the acting head of Department as at the time of writing this thesis, Dr. F. A. Oladeji, a true sister and friend, not only for always giving me the push to do more and meet deadlines but also for always being ready to sit

with me to dot my i's and cross my t's; Dr. E. P. Fasina, my brother from Ijebu, for his encouragement and useful counsels; Dr. A. O. Sennaike, for his assistance in my data pre-processing and contributions to my seminar write-ups; Dr. V. Odumuyiwa for his support and useful comments and contributions; Dr. O. B. Okunoye and Dr. A. U. Rufai, my paddies and 'thesis consultants', for being ever-ready to point and nudge me in the right direction on this journey; Dr. B. A. Sawyerr for his support and objective criticisms always; Dr. N. A. Azeez, my relevant-publications "broker" for always assisting in getting full text of relevant publications at no cost to me; Mr. L. Ikuvwerha for his support and brotherly love; Mrs. R.A. Ajetunmobi, my sister and roommate, for her support, love and pampering of me; also, Dr. C. Yinka-Banjo, Mrs. C. Ojiako, Ms. R. Isimeto, Mrs. D.T. Afolabi, Mr. S. E. Edagbami, Mr. O. O. Ajayi, and my colleague on the programme, Dr. A. M. Adegoke, for their friendship and support.

I, also, appreciate the support and contributions, in one way or the other, of the non-teaching staff of the Department, Mrs. Toyin Aloku, Mrs. Idowu, Mrs. Alayaki, Mrs. Bamgbelu, Mrs. Emeana, Mrs. Oluwamuhuru, Alhaja Gbolahan, Miss Nonye Nbonu, Mr Isaiah Ayandele, Mr. Olaitan and the other technical staff. Together with the academic staff, these people created an enabling environment for me to successfully complete this programme.

My sincere appreciation also goes to the following persons in the University of Lagos community for their immeasurable support at the concluding stage of this programme: Dr. A. O. Akala, Dr. Luqman Adeoti, Dr. Fashanu, Dr. Agunsoye, Dr. Adeyanju Sosimi, Dr. Kehinde Orolu and paddies at the CITS, in persons of Mr. Ore, Faisal, Seun and others, for always being there to solve my hardware and software challenges.

My sincere gratitude also goes to the members of Octagon '90 Club of University of Lagos and the members of the Great Table of Senior Staff Club of University of Lagos for providing me with necessary social distraction while on campus.

My sincere appreciation goes to my family, the Agbomola clan. Having you guys beside me, behind me and around me makes all the difference especially my brother, Quadri (a.k.a. Hero). Guy, the years we spent together on campus were my best years while on the programme. To my son - Iyioluwa, daughter - Abiodun, nieces and nephews and also my marvellous in-laws especially Pastor Adeemola Alebiosu, Alhaji Adebayo Adesanya and Mrs. Bukky Alli (a.k.a. Royal Mother), I say thank you.

I will also like to acknowledge the immense contributions of the following people to the person I have become today: My wonderful old and bosom friends who stood by me through thick and thin, Dr. and Major (Mrs.) Sola Oloyede, Mr. and Alhaja Lookman Oseni, Mr. and Mrs. Sina Mustapha, Pastor (Mrs.) Adenike Adesanya, Ronke Raji, Adedoyin Adenuga, Mrs. Bunmi Lawal-Olugbodi; my special friends, well-wishers and destiny-helpers who cheered me on: Honourable Gbolahan O. Yishawu (GOY), Elder Sina Olukanni, Mr. Joshua Kuje, Mrs. Dora Efunshile, and others that space would not allow me to list.

Also, I will like to put on note the love, encouragements and support from my colleagues who are my friends and lovers of my well-being and continued progress in persons of Mrs. Olanrewaju Ijaola, Dr. Uduak Aletan, Dr. A. M. Petu-Ibikunle, Dr. Bolupe Awe, etc. and, of course, not forgetting my brother and neighbour, Mr. Olusoji Awojobi.

I also acknowledge the support of the management of National Open University of Nigeria for granting me study leave to complete this programme and Prof. Femi Peters, who sowed the seed of my application for the leave, for his encouragement and support all through the programme.

My sincere and unalloyed gratitude also goes to the wonderful people that I have met and related with at one point or the other in this walk called life. Whether you realise it or not, you have all contributed to my becoming who I am today.

ABSTRACT

Global interconnectivity of systems has left inter-networked systems vulnerable to various forms of complex attacks. Researchers continue to work on new ways, which includes proactive ones of securing such systems, in order to eradicate or minimise security threats. One of such attempts is network attack prediction systems. Distributed Denial of Service (DDoS) attack is a class of network attack that can span several continents. It floods the computer network with heavy loads of unwanted packets and requests that weigh down the system resources such as memory and processors. Hidden Markov model (HMM) is one of the models that can be used to predict and detect such attacks. Issues associated with the use of HMM are determination of the hidden and observable states and subsequently, the model parameters estimation since the performance of the model depends on the accurate selection of these parameters. Related issue is the need to overcome long training time of the traditional HMM algorithm especially during model construction as well as ensuring that the learning algorithm does not converge to a local maximum. This study presents a novel parsimonious HMM-based model in which the entropy-based values of the network traffic features and the Distributed Denial of Service (DDoS) attack phases form the observable and the hidden states of the model, respectively. Entropy and *K*-Means clustering were deployed respectively to determine the observable and hidden states that characterise the HMM. In order to improve computational efficiency of the algorithm for estimating the parameters of the model, Kullback-Liebler Divergence (KLD) method was employed for reducing and selecting appropriate parameters to achieve a good prediction model. Variational Bayesian Inference (VBI) was employed in optimising the HMM. The performance of the model was evaluated through experiments using DARPA 2000 Intrusion Specific dataset, DARPA 1999 dataset and CAIDA 2007 simulated real time DDoS attack data. The experimental results when compared with an existing work, where Markov Chain was used, show that the model gives faster and higher prediction accuracy for predicting DDoS attack. Specifically, the prediction accuracy, false positive rate and false negative rate show 10%, 11% and 9% improvement, respectively while the computational time was reduced by 42%.

Keywords*:* DDoS, Network intrusion, Variational Bayesian inference, Hidden Markov model, Kullback-Liebler divergence.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ALGORITHMS