

Enhanced Moving Target Defense Mechanisms to Handle Cyber Attacks

By

M. UMA

(10PH076)

Supervisor

Dr. G.PADMAVATHI

A Thesis Submitted to

Avinashilingam Institute for Home Science and Higher Education

for Women, University, Coimbatore - 641 043

In partial fulfilment of the requirements for the degree of

DOCTOR OF PHILOSOPHY

IN

COMPUTER SCIENCE

June 2014

ACKNOWLEDGEMENTS

First and foremost, I am extremely thankful to the **LORD ALMIGHTY** for his graces and blessings bestowed on me.

I would like to place on record my reverential gratitude to **Late Ayya Dr. T. S. Avinashilingam Avl.**, Founder and President and First Chancellor of Avinashilingam University for Women, Coimbatore for providing the temple of learning and also for his heavenly blessings. I also owe my sincere and humble gratitude to **Late Amma Dr. Rajammal P. Devadas Avl., M.A., M.Sc., Ph.D.** Former Chancellor, Avinashilingam University for Women, Coimbatore

I record my sincere thanks to **Late Anna Mr. T. K. Shanmuganandam, B.A.,B.L.**, Former Chancellor, Avinashilingam University for Women, Coimbatore for providing the platform to carry out the research.

I record my sincere thanks to **Dr. T. S. K. Meenakshi Sundaram**, Chancellor, Avinashilingam University for Women, Coimbatore for providing the infrastructure for the conduct of the research.

I express my sincere and heartfelt thanks to **Dr. Sheela Ramachandaran, M.Sc., PG. Dip., Ph.D.**, Vice Chancellor, Avinashilingam University for Women, Coimbatore for providing necessary facilities and resources for the successful completion of this research work.

I express my sincere thanks to **Dr. Saroja Prabhakaran, M.A., Dip. Ed, Ph.D.**, Former Vice Chancellor, Avinashilingam University for Women, Coimbatore for motivating me to carryout the research, the constant encouragement, timely help, care and advice throughout the research.

I extend my gratitude to **Dr. Gowri Ramakrishnan, M.Sc., M.Phil., Ph.D.**, Registrar, Avinashilingam University for Women, Coimbatore for providing the infrastructure for the conduct of the research.

I express my heartfelt thanks to Dr. **P. Santhanakrishnan**, Director, Research and Consultancy, Avinashilingam University for Women, Coimbatore, for giving an opportunity to do research work.

I express my sincere and heartfelt thanks to **Dr. R. Parvatham M.Sc., Dip.Ed., M.Phil., Ph.D.**, Former Dean, Faculty of Science, Avinashilingam University for Women, Coimbatore for her spontaneous and timely help and amenities provided for the successful completion of this research work.

I also record my thanks to **Dr. Mrs. Parvathi**, Dean, Faculty of Science, University for Women, Coimbatore for motivating me to carryout the research, the constant encouragement, care and advice throughout the research.

I feel extremely privileged and fortunate to have worked under the able guidance and professional supervision of my guide, **Dr. G.PADMAVATHI, M.Sc., M.Phil., Ph.D.**, Professor and Head, Department of Computer Science, Avinashilingam University for Women, Coimbatore. Her constant encouragements, motivation, valuable and constructive suggestions and untiring support have guided me to gain and explore deep knowledge in the research field.

She helped me to define my research goals and showed the way to achieve them. Her able guidance, systematic approach guided me to put my best possible efforts in completing my work and documentation. Her sympathetic friendly nature, timely counseling, willingness to help at anytime, anywhere and at any situation during the entire period of the study have molded this research into a reality.

I record my gratitude to all **Ph.D and M.Phil Research Scholars, Faculty members** of Department of Computer Science, **Researchers** working in sponsored projects and **Staff Members** of Computer Center, Avinashilingam University for Women, Coimbatore for their encouragement and support.

I also thank My Mother **Mrs.M.Malliga**, My Brother **Mr.M.Arunkumar**, My Grandma **Mrs.D.SriRengathammal**, My Uncle **Mr.Alpandi Kannan** and **Mr.T.Jeyaraman**, My cousin **Mr.R.Praveen Kumar**, **Mr.M.Rangaraj** and **Mr.D.Augustin**, My Sister **Mrs.M.Chitra**, My brother-in-law **Mr.Anantharaj Apisek**, My Nephew **Master.N.Swaraj Kanna**, **Master.Abinesh Peter Solomon** and **Master.Adriel Jebi**, My Niece **Miss.N.Yadavi**, My Friend **Mr.P.Prem Kumar**, **Ms.R.KalpanaBharathi** and **my entire family** for their patience, wishes, prayers, encouragement and constant support extended to me at all the times throughout my career. I also thank all my **Friends, Relatives** and My well wishers **Dr.S.Chidambaranathan** and **Mr.N.Kumar** for their support and encouragement.

M. UMA

ABSTRACT

Secure communication in networking is still an open challenge due to the rapid development in technology. The increased use of networking makes the communication vulnerable to active and passive attacks. The decisive aim of the security is to maintain Confidentiality, Availability, Integrity, Non- repudiation and Authentication. According to a 2012 survey, that every organization is experiencing with an average of 102 attacks every week.

Based on the literature review, it is observed that efficient defense mechanisms are essential to defend against known and unknown cyber attacks. Game changing approaches are suggested as a defense mechanism to handle such attacks. The three game changing approaches namely, Trusted Tailored Spaces, Moving Target Defense Mechanisms and Cyber Economics are suggested as Research and Development Essentials. Among the three, moving target defense mechanisms are not explored much and only a few of them are used to handle attacks.

Moving target is a dynamic concept as it confuses the attackers by moving the real target often based on time or event. In the National Cyber Leap Year Summit Participants Report 2009, there are 11 moving target defense mechanisms suggested. According to the co-chairs' report, four moving target defense mechanisms are taken for study in this research work.

The objectives of the thesis are to Improve the quality of service in terms of End-to-end delay, Latency, Packet delivery ratio, Throughput, Reduce the number of retransmissions of data packets, Save time, Improve the accuracy of detection, Appropriate security application and Enhance storage security.

Few solutions are studied and enhanced. The proposed traffic monitoring technique achieves increased efficiency in traffic monitoring, adaptability for various network sizes, reduced retransmission and time saving. Cyber attack detection is done using the enhanced dimensionality reduction technique and the

outcome is improved accuracy in detection of known cyber attacks. The percentage of detection rate is 94%

For unknown cyber attack detection, four moving target defense mechanisms are implemented and improvised. They are Smart Motion Adaptation/Management - Game Theory, Robust Cryptographic Authentication - Mouse Dynamics, Data Chunking and Decentralization and Decoys. The above moving target defense mechanisms are enhanced to achieve the objectives of the thesis.

The secured hash based game theory approach is proposed. The experimentation is conducted using the NS2 simulator and the performance is estimated in terms of reduced end to end delay, increased packet delivery ratio, throughput. The proposed method also ensures neighbor authentication. The cyber attack detection rate is 71%.

Enhanced mouse dynamics is another method which outperforms the existing method in terms of reduced authentication time, reduced false acceptance rate, reduced false rejection rate and increased accuracy in detection of unauthorized users. The detection accuracy is observed to be 73%. The proposed application is developed using JAVA 1.7 as front end and mysql as back end.

The improved data chunking using non-sequential storage has showed better performance than the existing method and it achieves development of an application, robust security and increased storage durability. It also achieves increased accuracy in detection of unknown cyber attacks. The percentage of detection rate is 79% when compared to Mark W. Storer method. The proposed application is developed using JAVA 1.7 as front end and mysql as back end.

The Integrated Time and Event Triggered approach is proposed and tested using Network Simulator NS2. Simulation results show that the proposed method performs better than the existing methods. The percentage of detection rate is 83%

It also achieves reduced end to end delay, increased packet delivery ratio and improved throughput.

From the experimental and simulation results, it is observed that the four proposed methods are robust against known and unknown cyber attacks.

TABLE OF CONTENTS

Chapter No.	Title	Page No.
I	INTRODUCTION	2
	1.1. Cyber Space	2
	1.2. Cyber Attacks	2
	1.3. Classification of Cyber Attacks	3
	1.3.1.Active Attacks	4
	1.3.2.Passive Attacks	4
	1.4. Cyber Attack Handling Mechanisms	5
	1.5. Problem Statement	7
	1.6. Problem Justification	7
	1.7. Secondary Objectives of the Thesis	8
	1.8. Significant Contributions	8
	1.9. Organisation of the Thesis	8
	1.10. Chapter Summary	9
II	REVIEW OF LITERATURE	11
	2.1 Network Traffic Monitoring	12
	2.2. Detection of known cyber attacks using Dimensionality Reduction Techniques	20
	2.3. Moving Target Defense Mechanisms	28
	2.3.1. Smart Motion Adaptation / Management – Game Theory	28
	2.3.2. Robust Cryptographic Authentication – Mouse Dynamics	31
	2.3.3. Data Chunking and Decentralization	35
	2.3.4. Decoys	37
	2.4. Observations due to literature	42
	2.5. Chapter Summary	43

Chapter No.	Title	Page No.
III	PROPOSED METHODOLOGY	45
	3.1. Research Design	45
	3.2. Contributions in each phase	48
	3.3. Chapter Summary	49
IV	NETWORK TRAFFIC MONITORING AND DETECTION OF KNOWN CYBER ATTACKS	50
	4.1. Network Traffic Monitoring	51
	4.2. Detection of Known Cyber Attacks	78
	4.3. Chapter Summary	84
V	SMART MOTION ADAPTATION/MANAGEMENT - GAME THEORY	
	5.1. Proposed Method using Enhanced Game Theory	87
	5.2. Phases of the Proposed Research Work	87
	5.2.1. Flow Diagram of the Proposed Method	88
	5.2.2. Steps Involved of this Research work	89
	5.3.3. Proposed Algorithm	91
	5.3. Performance Metrics	91
	5.4. Simulation Environment	92
	5.5. Results and Discussions	93
	5.6. Chapter Summary	98
VI	ROBUST CRYPTOGRAPHIC AUTHENTICATION - MOUSE DYNAMICS	
	6.1. Proposed Research work using Enhanced Mouse Dynamics	100
	6.2. Phases of the Research Work	100
	6.2.1. Flow Diagram of the Proposed Method	101
	6.2.2. Main Steps of the Enhanced Method	101
	6.2.3. Algorithmic steps of the Proposed Research work	103
	6.3. Performance Metrics	103
	6.4. Results and Discussions	104

Chapter No.	Title	Page No.
	6.5. Chapter Summary	105
VII	IMPROVED DATA CHUNKING USING NON-SEQUENTIAL STORAGE	
	7.1. Proposed Method using Improved Data Chunking	107
	7.2. Phases of this Research work	108
	7.2.1. Flow Diagram of this Research Work	108
	7.2.2. Steps Involved in this Research Work	110
	7.2.1.1. Registration and Key Generation	111
	7.2.1.2. Attack Detection using Markov Chain Model	113
	7.2.1.3. Chunking Process	114
	7.2.1.4. Encryption Process	114
	7.2.1.5. Proposed Non-Sequential Storage	115
	7.2.3. Proposed Algorithm	117
	7.3. Performance Metrics	117
	7.4. Simulation Environment	118
	7.5. Results and Discussions	118
	7.6. Chapter Summary	120
VIII	ENHANCED DECOYS WITH INTEGRATED TIME AND EVENT TRIGGERED APPROACH	
	8.1. Proposed Integrated Time and Event Triggered Approach	122
	8.1.1. Phases of this Research Work	123
	8.1.1.1. Steps Involved of the Integrated Method	
	8.1.1.2. Flow diagram of the Proposed Method	
	8.1.1.3. Proposed Algorithm	
	8.1.2 Performance Metrics	130
	8.1.3 Simulation Environment	131
	8.1.3.1. Simulation Parameter	
	8.1.4 Results and Discussions	131
	8.2. Evaluation of the Proposed Method	135
	8.3. Chapter Summary	136

Chapter No.	Title	Page No.
IX	CONCLUSION AND FUTURE DIRECTIONS	
	9.1. Summary and Conclusion	137
	9.2. Future Research Directions	139

LIST OF FIGURES

Figure No.	Title	Page No.
1.1	Cyber Attack Classification	
1.2	Cyber Attack Handling Mechanisms	
2.1	Classification of Network Traffic Monitoring Techniques	
2.2	Communication between the Manager and Agent	
2.3	Dimensionality Reduction Techniques	
3.1	Major Steps Involved in the Research Methodology	
3.2	Consolidated view of the Proposed Research Methodology	
3.3	Conceptual view of the Improved Moving Target Defense Mechanisms	
3.4	Processing steps of Proposed Network Traffic Monitoring Technique	
3.5	End to End Delay for Network Surface Area – 200m x 200m up to 1500m x 1500 m based on Data Transfer Rate	
3.6	Packet Loss for Network Surface Area – 200m x 200m up to 1500m x 1500m based on Data Transfer Rate	
3.7	Throughput for Network Surface Area – 200m x 200m up to 1500m x 1500m based on Data Transfer Rate	
3.8	End to End Delay for Network Surface Area – 200m x 200m up to 1500m x 1500m based on Time(Seconds)	
3.9	Packet Loss for Network Surface Area – 200m x 200m up to 1500m x 1500m based on Time(Seconds)	
3.10	Throughput for Network Surface Area – 200m x 200m upto 1500m x 1500m based on Time(Seconds)	
3.11	Simulation Parameter with different secure routing protocol – DSR	
3.12	Simulation Parameter with different secure routing protocol – TORA	

Figure No.	Title	Page No.
3.13	Simulation Parameter with different secure routing protocol – OLSR	
3.14	Simulation Parameter with 20 Nodes	
3.15	Simulation Parameter with 40 Nodes	
3.16	Simulation Parameter with 60 Nodes	
3.17	Simulation Parameter with 80 Nodes	
3.18	Simulation Parameter for 20 Nodes using VBR Traffic Model	
3.19	Simulation Parameter for 40 Nodes using VBR Traffic Model	
3.20	Simulation Parameter for 60 Nodes using VBR Traffic Model	
3.21	Simulation Parameter for 80 Nodes using VBR Traffic Model	
3.22	Simulation Parameter for 100 Nodes using VBR Traffic Model	
3.23	Enhancement of PCA with SVM	
3.24	Cyber Attack Detection by PCA	
3.25	Cyber Attack Detection by LDA	
3.26	Cyber Attack Detection by ICA	
3.27	Cyber Attack Detection by PCA using Enhanced PCA with SVM	
4.1	Key Generating Process of SHA-512	
4.2	Processing Steps of AES Algorithm	
4.3.	Flow diagram of the Improved Data Chunking	

LIST OF TABLES

Table No.	Title	Page No.
2.1.	Algorithmic Steps of SNMP	15
2.2	Algorithmic Steps of RMON	16
2.3	Algorithmic Steps of Netflow	18
2.4	State-of-the-art – Data Chunking	29
2.5	State-of-the-art – Decoys	33
2.6	State-of-the-art – Mouse Dynamics	37
2.7	State-of-the-art – Game Theory	41
3.1	Improved SNMP Algorithm	52
3.2	Simulation Parameters	54
3.3	Numerical Comparison Results of the Performance Metrics	85
3.4	Algorithm for Enhanced PCA with SVM	89
4.1	Proposed Algorithm of Improved Data Chunking	103
4.2	Results of FAR and FRR for every 50 users	104
4.3	Cyber Attack Detection Rate	105
4.4	Detection Rate of infected files by the Proposed Method	105
5.1	Packet Header Format of the Proposed Method	109
5.2	Proposed Algorithm of Integrated Time and Event Triggered Approach	114
5.3	Simulation Parameters	117
5.4	Comparative results of the Proposed Method	118
5.5	Cyber Attack Detection Rate	118
6.1	Proposed Algorithm	124
6.2	Comparative Results of FAR, FRR and Authentication Time	125

6.3	Cyber Attack Detection Rate	125
7.1	Notations used in Proposed Method	128
7.2	Proposed Algorithm	135
7.3	Simulation Parameter	136
7.4	Results of Throughput	137
7.5	Results of Overhead	137
7.6	Results of Packet Delivery Ratio	138
7.7	Results of End to End delay	138
7.8	Results of Packet Drop	139
7.9	Results of Average No. of Claims (Based on Time)	140
8.1	Evaluation Results of the Proposed Methods	141

ACRONYMS

QoS	Quality of Service
DoS	Denial of Service
SNMP	Simple Network Monitoring Protocols
RMON	Remote Monitoring
PCA	Principal Component Analysis
LDA	Linear Discriminant Analysis
ICA	Independent Component Analysis
CLP	Conditional Legitimate Probability
DDoS	Distributed Denial-of-Service
PCANNA	Principal Component Analysis Neural Network Algorithm
ROC	Receiver Operating Characteristic
FAR	False Acceptance Rate
FRR	False Rejection Rate
NDN	Named Data Networking
ICN	Information-Centric Networking
IPCA	Incremental Principal Component Analysis
HMM	Hidden Markov Model
DR	Data Representation
WLAN	Wireless Local Area Network
RMTI	Routing with Metric-based Topology Investigation
RIPv2	Routing Information Protocol
TTCAN	Time Triggered Controller Area Network
RODL	Round Description List
ET	Externally Triggered
IT	Internally Triggered
FOTG	Fault-Oriented Test Generation
SHARP	Sharp Hybrid Adaptive Routing Protocol

AODV	Ad hoc On-Demand Distance Vector
ECC	Elliptic Curve Cryptography
SVM	Support Vector Machine
SHA-512	Secured Hash Algorithm
AES	Advanced Encryption Standard
CDC	Content Defined Chunking
DSR	Dynamic Source Routing
TORA	Temporally Ordered Routing Algorithm
OLSR	Optimized Link State Routing Protocol
CBR	Constant Bit Rate
VBR	Variable Bit Rate
RIP	Routing Information Protocol
OSPF	Open Shortest Path First