العنوان:	Development and Implementation of fast Network Intrusion Detection Systems
المؤلف الرئيسي:	Mahmoud, Mohamed Awad Mohamed
مؤلفين آخرين:	Mohamed, Mohamed Abd Alazim، Abd Alfattah, Abd Alfattah Ibraheem، Tolba, Ahmed Said(Super.، Super)
التاريخ الميلادي:	2012
موقع:	المنصورة
الصفحات:	1 - 192
رقم MD:	536381
نوع المحتوى:	رسائل جامعية
اللغة:	English
الدرجة العلمية:	رسالة دكتوراه
الجامعة:	جامعة المنصورة
الكلية:	كلية الهندسة
الدولة:	مصر
قواعد المعلومات:	Dissertations
مواضيع:	لكشف الدخلاء، جرائم المعلومات، شبكات الحاسب
رابط:	https://search.mandumah.com/Record/536381

تكنولوجيا نظم كشف أو مراقبة البيانات المتسللة من/إلى شبكات الحاسب الألى واحده من أكثرالتكنولوجيات أهمية في حماية الشبكات و الذى يعمل بامتزاج مع الجدار الناري, Firewall . بحكم أن في وقتنا الحاضر قد ازداد الاحتكاك بالإنترنت حيث أصبح الركن الأساسي في الاتصال بالعالم الخارجي و ايضا حاجة الشركات -بغض النظر عن حجمها- بالسماح للموظفين أو للعملاء أيضا بالدخول إلى الشبكة الداخلية للشركة أو حتى اتصال الشركة نفسها بفروعها في أماكن مختلفة , فقد أصبح لزاما تحديد المناطق أو الأفراد الموثوق بهم و مع ذلك فإن الموضوع تعقد إلى أن المشكلة أصبحت ليست فقط تحديد مواطن الثقة بل أيضا كيفية التأكد من هذه الجهة الموثوق بها أو بمعنى أخر كيف أحمي نفسي أيضا ممن أثق بهم!! , صاحب تقديم هذه الخدمة هو نظام كشف التسلسل IDS. إكتشاف الأختراق تلقى اهتماما كبيرا من جانب كل من الصناعة والأوساط البحثية و سبب هذا الاهتمام هو الخسائر الهائلة التى تنتج عن أختراق وتسريب او تدمير المعلومات وأيضا براعة ومهارة المخترقين حيث انهم يقومون بتحديث وسائل وطرق الاختراق. أيضا التطور السريع فى سرعة تداول المعلومات على شبكات الحاسب الألى أدى الى ضرورة تطوير سرعة أنظمة إكتشاف الأختراق لتواكب سرعات التدفق العالية على تلك الشبكات.

لأختبار أى تقنية مبتكرة كان حتما واجب أختبارها على شبكة حقيقية ولاكن بات هذا صعبا لعدة أسباب من أهمها احتمال توقف مؤقت للشبكة قد يؤثر على سير العمل الذى قد يكون خطيرا أو

حرجا وأيضا اذا لم يحدث ذلك فقد تكون هناك معلومات سريه مثل كلمة السر وأسماء المستخدمين لا يستوجب الاطلاع عليها من قبل أفراد فريق الأختبار. كل هذا اجبر المجتمع البحثى على توفير قواعد بيانات تسهل على الباحثين تنفيذ أبحاثهم وكان من أشهرها DARPA Dataset و KDD'99 Dataset.

الخوازميات المطبقة فى هذا البحث تم تنفيذها باستخدام مصفوفة البوابات المبرمجة حقليا (FPGA) للإستفادة من المميزات التي توفرها كسرعة الأداء لتتوافق مع السرعات العالية لتتدفق المعلومات على شبكات الحاسب الألى وقابليتها للبرمجة أكثر من مرة لتتوافق مع التحديثات المستمرة فى أنواع وأساليب الأختراقات. FPGA تعني مصفوفات البوابات المنطقية القابلة للبرمجة، وهي عبارة عن دوائر متكاملة تتكون من صفوف من البوابات المنطقية كل بوابة يمكن التحكم في نوعها وتحويلها من نوع الى أخر مثلا من AND الىNAND ومنNOR الىNOT الى أخره ويمكن أيضا التحكم في توصيل كل بوابة بالبوابات الاخرى فيمكن عمل التوصيل الذي نريده ويمكن بذلك تحويل الدائرة المتكاملة من نوع الى أخر عن طريق البرنامج الخاص ببرمجتها. وهى تستخدم في التطبيقات التي تحتاج الى تغيير دوائرها باستمرار وبينما كان ذلك صعبا في الماضي فانه الان يمكن أن يحدث بمجرد انزال برنامج جديد يغير من تركيب الدائرة.

ويهدفِ البحث إلي: (أ) مُنَاقَشَة تقنياتِ إكتشاف الأختراق, (ب) محاولة التغلب على التحديات التى تواجه هذه التقنياتِ (ت) تَطوير أساليب جديده لأكتشاف الأختراق, , (ث)

تَطبيق أكتشاف الأختراق باستعمال VHDL و (ج) تنفيذ أفضل تقنيات أكتشاف الأختراق بإستخدام مصفوفة البوابات النطقية المبرمجة حقلياً (FPGA).

و تنقسم الرسالة إلى سبعة أبواب و ملحقين كما يلي:

الفصل الأول: تحت عنوان "Introduction" و هو مقدمة تاريخية عن الإختراق المعلوماتى وطرق أكتشافه على مدار العقود الما ضية وأهداف واسهامات الرساله واخيرا التقسيمه الاساسيه فى الرساله.

الفصل الثاني: تحت عنوان "Network Security: An Overview" وفيه تم عرض مقدمه عن أنظمة تأمين الشبكات وخدمات وأليات الأمن المعلوماتى على شبكات الحاسب الألى وأخيرا عرض لأدوات تأمين شبكات الحاسب الألى والتى من ضمنها مكتشف الإختراق IDS.

الفصل الثالث: تحت عنوان "Intrusion Detection Systems Overview" وفيه تم عمل أستعراض كامل لنظام إكتشاف الإختراق من حيث تعريفه ومكان تواجده فى الشبكة المطلوب حمايتها ومكانه بالنسبه للجدار النارى وأيضا الأجزاء المكونه له وأخيرا قدم الفصل طرق تنفيذ أنظمة إكتشاف الأختراق المختلفة.

الفصل الرابع: تحت عنوان "Conventional IDS Systems " في هذا البحث تم تنفيذ ثمانية أنواع من خوازميات الشبكات العصبية في محاولة لتحديد ماأذا كان التدفق تدفق طبيعي أو تدفق فيه إختراق وأذا كان به إختراق فماتصنيف هذا الإختراق وما أسمه حيث أن هذا يُسهل لمدير النظام اتخاذ اجراء مناسب حيال هذا الإختراق. أيضا تم تنفيذ أثنين من خوارزميات التنقيب المعلوماتي وهما Decision Tree و Naïve Bayes لتحقيق نفس الهدف. نتائج ما سبق أظهرت أن الخوارزميات السابقة لها قدرة كبيرة على أكتشاف ماأذا كان هناك إختراق ام لا ولكن تحديد تصنيفه وأسمه فما زالت مهمة صعبة.

الفصل الخامس: تحت عنوان "The Proposed IDS Systems " هذا ماتم تقديمه في هذا البحث حيث قدم فكرة مستواحة من تطبيق مُكتشف متعدد المراحل/مختلط من الأنواع التقليدية السابق تنفيذها في الباب السابق. هذا الأسلوب استطاع بنجاح التعرف على جميع أصناف الأختراق بالإضافة الى التعرف على جميع أنواع أسماء الإختراقات. البيانات المستخدمة تعتبر ضخمة جدا ولتسهيل عملية تنفيذ الخوازميات السابقة كان لابد من تنفيذ عمليات ضغط وإختصار لتلك المعلومات من الناحية الكمية وذلك بإزالة البيانات المتشابهة

أو من الناحية الكيفية بإختصار عناصر البيانات إما بإختيار أهم تلك العناصر أو دمجها مع بعضها وإستنباط عناصر جديدة وتم الآستقرار على طريقة تحليل المكونات الرئيسية Principal Components Analysis PCA التي قلصت الـ41 عنصر المكون للتدفق الواحد في قاعدة البيانات الى 22 عنصر.

الفصل السادس: تحت عنوان "Hardware Implementation of IDS " يحتوي هذا الفصل على تنفيذ بعض الأساليب المقترحة الجديدة في الفصل السابق على شريحة مصفوفة البوابات المبرمجة حقليا FPGA للإستفادة من المميزات الهائلة التي توفرها وخصوصا في سرعة الأداء. أيضا تم تنفيذ منظومات متعددة المراحل منهم مستهدفه التعرف على صنف الهجوم. عملية التنفيذ على الشريحة واجهت صعوبات عديدة منها ضيق المساحه المتاحه على الشريحه وطرق تداول البيانات على الشريحه وأيضا تنفيذ الدالة الغير خطية المستخدمة في الخلية العصبيه المكونه للشبكة العصبيه كل هذة الصعوبات تم التغلب عليها بنجاح حيث تم ضغط الـ 22 عنصر السابق التحدث عنهم في الفصل الثامن الى عدد عناصر أقل. الضغط كان مبني على إستبعاد قيم الـ PCs ذات الأقل مرتبة مع الاحتفاظ بنسبة تعرف

عاليه. قدم هذا الفصل دالة جديدة لتمثيل الدالة الأصلية الغير خطيه السابق الحديث عنها ولكنها كانت صعبة التنفيذ لوجود عملية قسمة فيها والتى تُغلب عليها بأستخدام دالة القسمة المتوفرة فى برنامج الشركة المنتجه للشريحة كملكية فكرية لها.

الفصل السابع: تحت عنوان " Conclusion " يحتوي هذا الفصل على ملخص الرسالة.

Abstract

Intrusion Detection Systems (IDSs) have recently received a blooming attention and interest from the scientific community as well as from the public. The interest from the public is mostly due to the recent events of terror around the world, which has increased the demand for useful security systems. There has been significant progress in improving the performance of computer-based intrusion detection systems algorithms over the last decade. Although algorithms have been tested and compared extensively with each other, there has been remarkably little work comparing the accuracy of computer-based IDSs with humans.

Our long term goal is to design and build an intelligent IDS that is accurate (low false negative and false positive rates), flexible, not easily fooled by small variations in intrusion patterns, adaptive in new environments, modular with both misuse and anomaly detection components, robust, able to detect known and unknown intrusions and real-time.

To achieve our goal, two phases of implementation were introduced; software and hardware phases. The software phase is divided into two sub-phases; the first introduces conventional IDS implementation which is based on neural networks and Data mining techniques. The results obtained were unsatisfactory. The second sub-phase introduces a proposed IDS which is based on hybriding and/or multistaging more than one conventional IDS. The proposed models were successfully able to detect all signatures and all classes of intrusions, in addition to the type of each stream (normal or attack) in the tested database. The first stage of

the multistage classifier is a perfect 2-types anomaly classifier, which ensures securing the network against attack (known and unknown attacks), whereas an alarm could be raised to the system administrator to take the proper action. Feature and topology reduction were one of most important challenges in this thesis due to massiveness of tested dataset and the huge structure of the implemented models. The proposed models were repeated with different neural networks topologies with simpler structure which are based on trial and error. Feature reduction process proceeds in two ways; record reduction by eliminating duplications and feature reduction. By applying Principal Components Analysis (PCA), the original 41-features were transformed to 22 ranked principal components (PCs) and the generated PCs were minimized by eliminating less ranked PCs until reaching a compromise situation between the smallest number of PCs and best detection efficiency.

As the demand on more network speed increases and new network protocols emerge, Network Intrusion Detection Systems (NIDSs) are increasing in importance and are being integrated in network processors. Currently, most IDSs are software running on a general purpose processor. Unfortunately, it is becoming increasingly difficult for software based IDSs to keep up with the increasing network speeds (10Gbps at backbone networks).This has underscored the need for the specialized hardware-based solutions which are portable and operate at wire speeds. Field Programmable Gate Arrays (FPGAs) are generic pieces of hardware

that can be reconfigured to perform any task. FPGA-based platforms can exploit the fact that the NIDS rules change relatively infrequently, and use reconfiguration to reduce implementation cost. In addition, FPGA-based systems can exploit parallelism in order to achieve satisfactory processing robustness.

To achieve robustness of IDS; FPGA-based IDSs were introduced, the hardware phase, based on neural networks and data mining intrusion detection techniques. Through MultiLayer preceptron (MLP) design, we faced common challenge in MLP hardware implementation which is tansig activation function which is difficult to implement due to its nonlinearity. Three techniques for tansig representation were presented, one based on Kwan approximation [172] and the other based on Piecewise Linear Approximation of a Nonlinear function (PLAN) approximation [173]. A third approximation, which is based on symbolic regression and genetic algorithm, is proposed. New challenge arisen in implementing the proposed tansig approximation which is the division process in FPGA. This was solved by using (Intellectual Property) IP CORE available in Xilinx ISE. FPGA-based IDSs, MLP and Decision Tree DT-j48 based, were implemented using two different programming strategies and data formats. Both techniques gave perfect results to detect normal and attack stream. Both implemented single stage IDS was followed by second stage which was able to detected stream's class after detecting stream's type.

العنوان:	Development and Implementation of fast Network Intrusion Detection Systems
المؤلف الرئيسي:	Mahmoud, Mohamed Awad Mohamed
مؤلفين آخرين:	Mohamed, Mohamed Abd Alazim، Abd Alfattah, Abd Alfattah Ibraheem، Tolba, Ahmed Said(Super.، Super)
التاريخ الميلادي:	2012
موقع:	المنصورة
الصفحات:	1 - 192
رقم MD:	536381
نوع المحتوى:	رسائل جامعية
اللغة:	English
الدرجة العلمية:	رسالة دكتوراه
الجامعة:	جامعة المنصورة
الكلية:	كلية الهندسة
الدولة:	مصر
قواعد المعلومات:	Dissertations
مواضيع:	لكشف الدخلاء، جرائم المعلومات، شبكات الحاسب
رابط:	https://search.mandumah.com/Record/536381

Contents

العنوان:	Development and Implementation of fast Network Intrusion Detection Systems
المؤلف الرئيسي:	Mahmoud, Mohamed Awad Mohamed
مؤلفين آخرين:	Mohamed, Mohamed Abd Alazim، Abd Alfattah, Abd Alfattah Ibraheem، Tolba, Ahmed Said(Super.، Super)
التاريخ الميلادي:	2012
موقع:	المنصورة
الصفحات:	1 - 192
رقم MD:	536381
نوع المحتوى:	رسائل جامعية
اللغة:	English
الدرجة العلمية:	رسالة دكتوراه
الجامعة:	جامعة المنصورة
الكلية:	كلية الهندسة
الدولة:	مصر
قواعد المعلومات:	Dissertations
مواضيع:	لكشف الدخلاء، جرائم المعلومات، شبكات الحاسب
رابط:	https://search.mandumah.com/Record/536381

Mansoura University
Faculty of Engineering
Electronic & Comm. Eng. Dept.

Development and Implementation of Fast Network Intrusion Detection Systems

A Thesis Submitted In Partial Fulfillment for the Requirements of

Ph.D. Degree
In
Electrical Communications Engineering

By

Eng. Mohamed Awad Mohamed Mahmoud
B.Sc. Electronic and Communications Engineering

Supervised by

Prof. Abdel-Fattah Ibrahim Abdel-Fattah
Professor at the Electronics and Communications Department-Faculty of Engineering-Mansoura University

Prof. Ahmed Said Tolba
Professor at Faculty of Computers and Information Sciences
Mansoura University

Dr. Mohamed Abdel-Azim Mohamed
Professor at the Electronics and Communications Department-Faculty of Engineering-Mansoura University

2012

Thesis Title:

Development and Implementation of Fast Network Intrusion Detection Systems

Researcher Name:
Mohamed Awad Mohamed Mahmoud

SUPERVISORS:

No.	Name	Position	Signature
1	Prof. Abdel-Fattah Ibrahim Abdel-Fattah	Department of Electronics and Communication Engineering Faculty of Engineering Mansoura University	
2	Prof. Ahmed Said Tolba	Professor at Faculty of Computers and Information Sciences- Mansoura University	
3	Prof. Mohammed Abdel-Azim Mohamed	Department of Electronics and Communication Engineering Faculty of Engineering Mansoura University	

Head of Dept.

Prof. Ahmed S. Samra

Vice Dean for Post Graduate Studies and Researches

Prof. Kasim Salah El-Alfy

Dean of the faculty

Prof. Mahmoud Mohamed Elmelegi

Thesis Title:

Development and Implementation of Fast Network Intrusion Detection Systems

Researcher Name:

Mohamed Awad Mohamed Mahmoud

Supervisors:

No.	Name	Position	Signature
1	Prof. Abdel-Fattah Ibrahim Abdel-Fattah	Department of Electronics and Communication Engineering Faculty of Engineering Mansoura University	
2	Prof. Ahmed Said Tolba	Professor at Faculty of Computers and Information Sciences- Mansoura University	
3	Prof. Mohammed Abdel-Azim Mohamed	Department of Electronics and Communication Engineering Faculty of Engineering Mansoura University	

Exam Committee:

No.	Name	Position	Signature
1	Prof. Abdel-Fattah Ibrahim Abdel-Fattah	Department of Electronics and Communication Engineering Faculty of Engineering Mansoura University	
2	Prof. Hassan H. Soliman	Department of Electronics and Communication Engineering Faculty of Engineering Mansoura University	
3	Prof. Wail Shawki Elkilani	Department of Computer Systems Faculty of Computers and Information -Ain Shams University	

Head of Dept.

Prof. Ahmed S. Samra

Vice Dean for Post Graduate Studies and Researches

Prof. Kasim Salah El-Ali

Dean of the faculty

Prof. Mahmoud Mohamed Elmelegi

بسم الله الرحمن الرحيم

" سُبْحَانَكَ لاَ عِلْمَ لَنَا إِلاَّ مَا عَلَّمْتَنَا إِنَّكَ أَنتَ الْعَلِيمُ الْحَكِيمُ "

صدق الله العظيم

(سورة البقرة- الآية 32)

Acknowledgement

First and foremost, I want to thank the source of every success to ***ALLAH;*** Next I am deeply thankful to my advisor Prof. Dr. Prof. ***Abdel-Fattah Ibrahim Abdel-Fattah*** who guided me through this entire journey.

I want to express my gratitude to Dr. ***Mohamed Abdel-Azim Mohamed,*** whose not only served as my supervisor but also encouraged, valuable guidance, indispensable help and challenged me throughout my academic program. His words of advice, his trust, and his patience and understanding helped me to reach this work. He has been a role model to me. He has always provided support whenever I need.

I owe my deepest gratitude and heartily thankful to my wife **and my daughters Mahy and Lara** whose accompanied me in every stage of this work with their patience, friendship, openness and their caring.

Special thanks to my family, my father, my mother, my sister, and my brothers whose support and unconditional help were invaluable in completing this work. Finally, I would like to seize the opportunity to thank all of you who make up an essential part of my life. Although not directly involved in this work, you have contributed to its completion in many ways.

Mohamed Awad

Abstract

Intrusion Detection Systems (IDSs) have recently received a blooming attention and interest from the scientific community as well as from the public. The interest from the public is mostly due to the recent events of terror around the world, which has increased the demand for useful security systems. There has been significant progress in improving the performance of computer-based intrusion detection systems algorithms over the last decade. Although algorithms have been tested and compared extensively with each other, there has been remarkably little work comparing the accuracy of computer-based IDSs with humans.

Our long term goal is to design and build an intelligent IDS that is accurate (low false negative and false positive rates), flexible, not easily fooled by small variations in intrusion patterns, adaptive in new environments, modular with both misuse and anomaly detection components, robust, able to detect known and unknown intrusions and real-time.

To achieve our goal, two phases of implementation were introduced; software and hardware phases. The software phase is divided into two sub-phases; the first introduces conventional IDS implementation which is based on neural networks and Data mining techniques. The results obtained were unsatisfactory. The second sub-phase introduces a proposed IDS which is based on hybriding and/or multistaging more than one conventional IDS. The proposed models were successfully able to detect all signatures and all classes of intrusions, in addition to the type of each stream (normal or attack) in the tested database. The first stage of

the multistage classifier is a perfect 2-types anomaly classifier, which ensures securing the network against attack (known and unknown attacks), whereas an alarm could be raised to the system administrator to take the proper action. Feature and topology reduction were one of most important challenges in this thesis due to massiveness of tested dataset and the huge structure of the implemented models. The proposed models were repeated with different neural networks topologies with simpler structure which are based on trial and error. Feature reduction process proceeds in two ways; record reduction by eliminating duplications and feature reduction. By applying Principal Components Analysis (PCA), the original 41-features were transformed to 22 ranked principal components (PCs) and the generated PCs were minimized by eliminating less ranked PCs until reaching a compromise situation between the smallest number of PCs and best detection efficiency.

As the demand on more network speed increases and new network protocols emerge, Network Intrusion Detection Systems (NIDSs) are increasing in importance and are being integrated in network processors. Currently, most IDSs are software running on a general purpose processor. Unfortunately, it is becoming increasingly difficult for software based IDSs to keep up with the increasing network speeds (10Gbps at backbone networks).This has underscored the need for the specialized hardware-based solutions which are portable and operate at wire speeds. Field Programmable Gate Arrays (FPGAs) are generic pieces of hardware

that can be reconfigured to perform any task. FPGA-based platforms can exploit the fact that the NIDS rules change relatively infrequently, and use reconfiguration to reduce implementation cost. In addition, FPGA-based systems can exploit parallelism in order to achieve satisfactory processing robustness.

To achieve robustness of IDS; FPGA-based IDSs were introduced, the hardware phase, based on neural networks and data mining intrusion detection techniques. Through MultiLayer preceptron (MLP) design, we faced common challenge in MLP hardware implementation which is tansig activation function which is difficult to implement due to its nonlinearity. Three techniques for tansig representation were presented, one based on Kwan approximation [172] and the other based on Piecewise Linear Approximation of a Nonlinear function (PLAN) approximation [173]. A third approximation, which is based on symbolic regression and genetic algorithm, is proposed. New challenge arisen in implementing the proposed tansig approximation which is the division process in FPGA. This was solved by using (Intellectual Property) IP CORE available in Xilinx ISE. FPGA-based IDSs, MLP and Decision Tree DT-j48 based, were implemented using two different programming strategies and data formats. Both techniques gave perfect results to detect normal and attack stream. Both implemented single stage IDS was followed by second stage which was able to detected stream's class after detecting stream's type.

List of Abbreviations

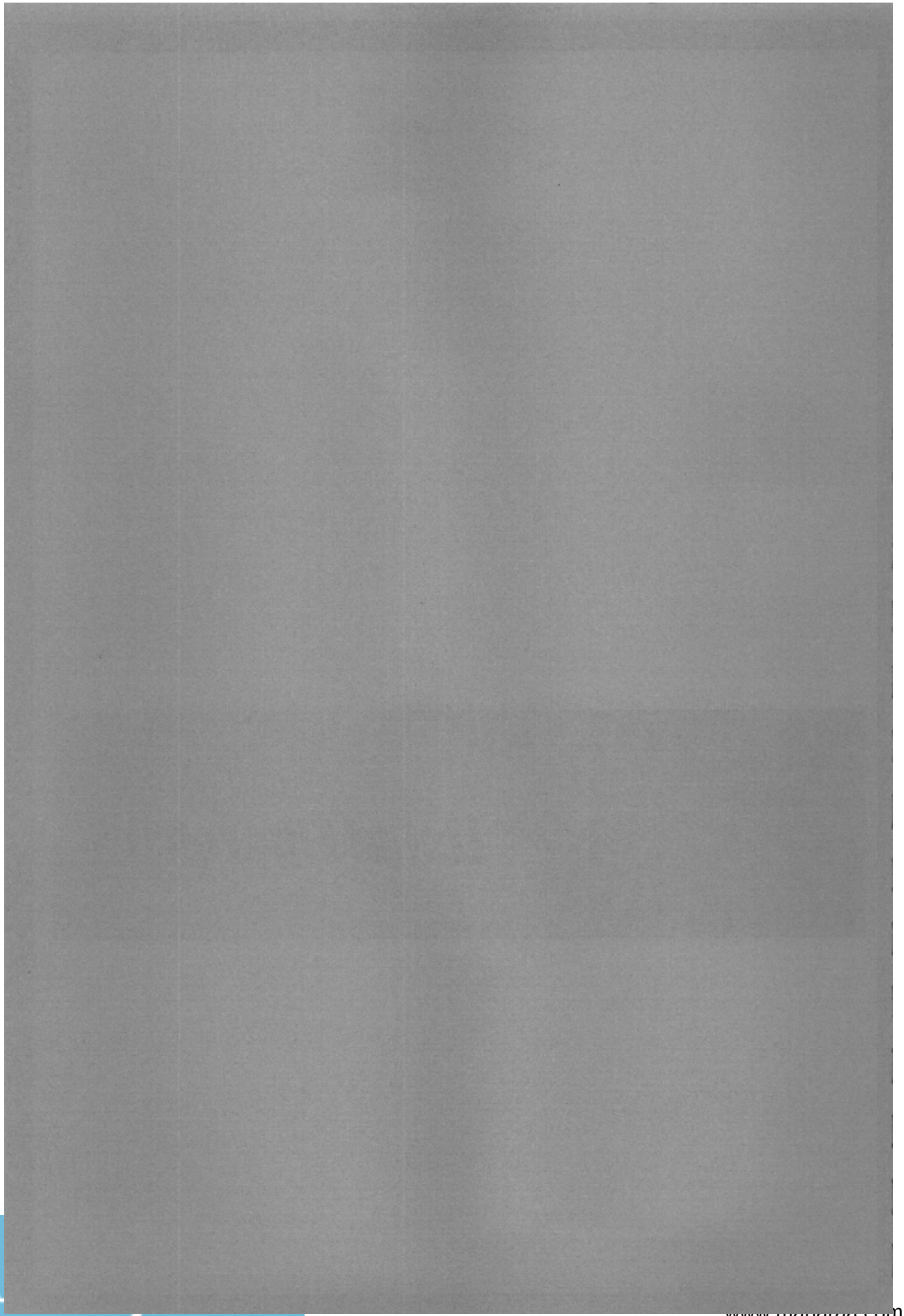
Symbol	Details
LMS	Least Mean Square rule
Login	Log in Unix command
ls	List Unix command
LVF	Las Vegas Filter
LVQ	Learning Vector Quantization
Madaline	Multiple ADAptive Linear Element
MADAM ID	Mining Audit Data for Automated Models for Intrusion Detection
MIB	Management Information Base
MIB	Management Information Base
MINDS	The Minnesota Intrusion Detection System
MIT	Massachusetts Institute of Technology
ML	Machine Learning
MLP	Multilayer Perceptron
MLS	Multi-Level Security
MNN	Modular Neural Network
NFR	Network Flight Recorder
NFS	Network File System
NID	Network Intrusion Detection
NNTP	Network News Transfer Protocol
NSM	Network Security Monitor
OSI	Open Systems Interconnection
PCA	Principal Component Analysis
PCs	principal components
PE	Processing unit (or Element)
PNN	Probabilistic Neural Network
POP	Post Office Protocol
ps	Active processes Unix command
R2L	Remote to Local
RBF	Radial Basis Function Networks
ReliefF	Recursive Elimination of Features
RFC	Request For Comments
RN	Recurrent Network
SATAN	Security Administrator Tool for Analyzing Networks
Simnet	simulation network

Symbol	Details
SMO	Sequential Minimal Optimization
SMTP	Simple Mail Transfer Protocol
SNMP	The Simple Network Management Protocol
SNMP	Simple Network Management Protocol
SNMPv1	Simple Network Management Protocol Version 1.
SNMPv2	Simple Network Management Protocol Version 2.
SNMPv3	Simple Network Management Protocol Version 3.
SOM	Self-Organizing Maps
SQ	SQuare
Sudo	Super User Do
SVMs	Support Vector Machines
TCB	Trusted Computing Base
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TCSEC	Trusted Computer System Evaluation Criteria
TDNN	Tapped Delay Neural Network
TDNN	Time Delay Neural Network
TELNET	TELecommunications NETwork
TLRNs	Time Lagged Recurrent Networks
TTL	Time To Live
U2R	User to Root
UDP	User Datagram Protocol

Symbol	Details
a.k.a. system logs	Authentication and Key Agreement
ADAM	Audit Data Analysis and Mining
ADC	Approximate Distance Clustering
AI	Artificial Intelligence
AIX	Advanced Interactive eXecutive
API	Application Programming Interfaces
ARP	Address Resolution Protocol
ASIC	Application-Specific Integrated Circuit
ATM	Asynchronous Transfer Mode
ATP	Advanced Technology Program
BSM	Basic Security Model
BSM	Basic Security Module
C2	Class 2
CAM	Content Addressable Memories
CANFIS	CoActive Neuro-Fuzzy Inference System
CERT	Computer Emergency Response Team
CFS	Correlation-based Feature Subset
CGI	Common Gateway Interface
CIDF	Common Intrusion Detection Framework
CM	Confusion Matrix
COPS	Computer Oracle and Password System
CPU	Central Processing Unit
CSI	Crime Scene Investigation
C-SVC	regularized support vector classification
DARPA	Defense Advanced Research Projects Agency
DFA	Deterministic Finite Automata
DIDS	Distributed Intrusion Detection System
DIDS	Distributed Intrusion Detection System
DNS	Domain Name System
DoS	Denial of Service
DR	Dimensionality Reduction
DT	Decision Tree
EMERALD	Electronic Management Research Library Database
EPT	Effective Process Time

Symbol	Details
FBI	Federal Bureau of Investigation
FCBI	Fast Correlation-Based
FPGAs	Field Programmable Gate Arrays
FS	Feature subset Selection
ftp	File transfer Protocol
FTPD	File Transfer Protocol Daemon
GA	Genetic Algorithm
GFF	Generalized Feed-Forward
Gido	Generalized intrusion detection objects
GrIDS	the Graph based Intrusion Detection System
GRNN	Generalized Regression Neural Network
GUI	Graphical User Interface
HMM	Hidden Markov Model
HTML	Hyper Text Markup Language
HTTP	HyperText Transfer Protocol
ICMP	Internet Control Message Protocol
ID3	Iterative Dichotomiser 3
IDDM	Intrusion Detection using Data Mining
IDES	Intrusion Detection Expert System
IDIOT	Intrusion Detection In Our Time
IDPSs	Intrusion Detection and Prevention System
IDSs	Intrusion Detection Systems
IP	Internet Protocol
IP	Intellectual Property
IPSs	Intrusion Prevention Systems
ISOA	Information Security Officer's Assistant
ISS's	Internet Security Systems
ITU-T	International Telecommunication Union Telecommunication standardization sector
JAM	Java Agents Metal-learning
JEN	Jordan/Elman Networks
KDDCUP' 99	Knowledge Discovery and Data mining tools competition
Klaxon	Klaxon audio signal
LAN	Local Area Network

List of Figures



List of Tables

العنوان:	Development and Implementation of fast Network Intrusion Detection Systems
المؤلف الرئيسي:	Mahmoud, Mohamed Awad Mohamed
مؤلفين آخرين:	Mohamed, Mohamed Abd Alazim، Abd Alfattah, Abd Alfattah Ibraheem، Tolba, Ahmed Said(Super.، Super)
التاريخ الميلادي:	2012
موقع:	المنصورة
الصفحات:	1 - 192
رقم MD:	536381
نوع المحتوى:	رسائل جامعية
اللغة:	English
الدرجة العلمية:	رسالة دكتوراه
الجامعة:	جامعة المنصورة
الكلية:	كلية الهندسة
الدولة:	مصر
قواعد المعلومات:	Dissertations
مواضيع:	لكشف الدخلاء، جرائم المعلومات، شبكات الحاسب
رابط:	https://search.mandumah.com/Record/536381

جامعـــة المنصـــورة
كليـــــة الهـــندســـة
قسم هنـدسة الإلكترونيات والإتصالات

تطوير وتنفيذ نظم سريعة لكشف الدخلاء علي شبكات الحاسب

توطئة للحصول على درجـــــة دكتوراة الفلسفة
فى هندســة الإتصالات الكهربيــة

رسالة مقدمـــــة من

المهندس / محمد عوض محمد محمود

بكالوريوس هندســة الإلكترونيات والإتصالات
كليـــة الهندســـــة – جامعة المنصـــــــــورة

إشـــــــــــــراف

أ.د. عبدالفتاح إبراهيم عبدالفتاح
أستاذ متفرغ بقسم هندسة الإلكترونيات والإتصالات
كليـــة الهندســـة – جامعة المنصـــورة

أ.د. أحمد سعيد طلبة
أستاذ بكلية الحاسبات ونظم المعلومات
جامعة المنصـــورة

د.م. محمد عبد العظيم محمد
مدرس بقسم هندسة الإلكترونيات والإتصالات
كليـــة الهندســـة – جامعة المنصـــورة

2012

Mansoura University
Faculty of Engineering
Electronic & Comm. Eng. Dept.

Development and Implementation of Fast Network Intrusion Detection Systems

A Thesis Submitted In Partial Fulfillment for the Requirements of

Ph.D. Degree
In
Electrical Communications Engineering

By

Eng. Mohamed Awad Mohamed Mahmoud
B.Sc. Electronic and Communications Engineering

Supervised by

Prof. Abdel-Fattah Ibrahim Abdel-Fattah
Professor at the Electronics and Communications Department-Faculty of Engineering-Mansoura University

Prof. Ahmed Said Tolba
Professor at Faculty of Computers and Information Sciences
Mansoura University

Dr. Mohamed Abdel-Azim Mohamed
Professor at the Electronics and Communications Department-Faculty of Engineering-Mansoura University

2012