


SpringerBriefs on Cyber Security Systems and Networks

Editor-in-chief

Yang Xiang, Digital Research & Innovation Capability Platform, Swinburne University of Technology, Hawthorn, Melbourne, VIC, Australia

Series editors

Liqun Chen , University of Surrey, Guildford, UK

Kim-Kwang Raymond Choo, Department of Information Systems and Cyber Security, University of Texas at San Antonio, San Antonio, TX, USA

Sherman S. M. Chow, Department of Information Engineering, The Chinese University of Hong Kong, Hong Kong

Robert H. Deng, School of Information Systems, Singapore Management University, Singapore, Singapore

Dieter Gollmann, Hamburg University of Technology, Hamburg, Germany

Javier Lopez, University of Malaga, Malaga, Spain

Kui Ren, University at Buffalo, Buffalo, NY, USA

Jianying Zhou, Singapore University of Technology and Design, Singapore, Singapore

The series aims to develop and disseminate an understanding of innovations, paradigms, techniques, and technologies in the contexts of cyber security systems and networks related research and studies. It publishes thorough and cohesive overviews of state-of-the-art topics in cyber security, as well as sophisticated techniques, original research presentations and in-depth case studies in cyber systems and networks. The series also provides a single point of coverage of advanced and timely emerging topics as well as a forum for core concepts that may not have reached a level of maturity to warrant a comprehensive textbook. It addresses security, privacy, availability, and dependability issues for cyber systems and networks, and welcomes emerging technologies, such as artificial intelligence, cloud computing, cyber physical systems, and big data analytics related to cyber security research. The mainly focuses on the following research topics:

Fundamentals and Theories

- Cryptography for cyber security
- Theories of cyber security
- Provable security

Cyber Systems and Networks

- Cyber systems Security
- Network security
- Security services
- Social networks security and privacy
- Cyber attacks and defense
- Data-driven cyber security
- Trusted computing and systems

Applications and Others

- Hardware and device security
- Cyber application security
- Human and social aspects of cyber security

More information about this series at <http://www.springer.com/series/15797>

Kwangjo Kim • Muhamad Erza Aminanto
Harry Chandra Tanuwidjaja

Network Intrusion Detection using Deep Learning

A Feature Learning Approach

 Springer

Kwangjo Kim
School of Computing (SoC)
Korea Advanced Institute of
Science and Technology
Daejeon, Korea (Republic of)

Muhamad Erza Aminanto
School of Computing (SoC)
Korea Advanced Institute of
Science and Technology
Daejeon, Korea (Republic of)

Harry Chandra Tanuwidjaja
School of Computing (SoC)
Korea Advanced Institute of
Science and Technology
Daejeon, Korea (Republic of)

ISSN 2522-5561 ISSN 2522-557X (electronic)
SpringerBriefs on Cyber Security Systems and Networks
ISBN 978-981-13-1443-8 ISBN 978-981-13-1444-5 (eBook)
<https://doi.org/10.1007/978-981-13-1444-5>

Library of Congress Control Number: 2018953758

© The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2018
This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.
The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.
The publisher, the authors, and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, express or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

This Springer imprint is published by the registered company Springer Nature Singapore Pte Ltd.
The registered company address is: 152 Beach Road, #21-01/04 Gateway East, Singapore 189721, Singapore

To our families for their lovely support.

Preface

This monograph presents recent advances in Intrusion Detection System (IDS) using deep learning models, which have achieved great success recently, particularly in the field of computer vision, natural language processing, and image processing. The monograph provides a systematic and methodical overview of the latest developments in deep learning and makes a comparison among deep learning-based IDSs. A comprehensive overview of deep learning applications to IDS followed by deep feature learning methods containing a novel deep feature extraction and selection and deep learning for clustering is provided in this monograph. Further challenges and research directions are delivered in the monograph.

The monograph offers a rich overview of deep learning-based IDS, which is suitable for students, researchers, and practitioners interested in deep learning and intrusion detection and as a reference book. The comprehensive comparison of various deep-learning applications helps readers with a basic understanding of machine learning and inspires applications in IDS and other cybersecurity areas.

The outline of this monograph is as follows:

Chapter 1 describes the importance of IDS in computer networks these days by providing a survey of a security breach in computer networks. It is highlighted that deep learning models can improve IDS performance. It also explains the motivation of surveying deep learning-based IDSs.

Chapter 2 provides all the relevant definition of IDS. It then explains different types of the current IDS, based on where we put the detection module and based on the used approach. Common performance metrics and publicly available benchmark dataset are also provided in this chapter.

Chapter 3 provides a brief preliminary study regarding classical machine learning which consists of supervised, unsupervised, semi-supervised, weakly supervised, reinforcement, and adversarial machine learning. It briefly surveys 22 papers which are using machine learning techniques for their IDSs.

Chapter 4 discusses several deep learning models which contain generative, discriminative, and hybrid approaches.

Chapter 5 surveys various IDSs that leverage deep learning models which are divided into four classes: generative, discriminative, hybrid, and deep reinforcement learning.

Chapter 6 discusses the importance of deep learning models as a feature learning (FL) approach in IDS researches. We explain further two models which are deep feature extraction and selection and deep learning for clustering.

Chapter 7 concludes this monograph by providing an overview of challenges and future research directions in deep learning applications for IDS.

Appendix discusses several papers of malware detection over a network using deep learning models. Malware detection is also an important issue due to the increasing number of malware and similar approach as IDS.

Daejeon, Republic of Korea
March 2018

Kwangjo Kim
Muhamad Erza Aminanto
Harry Chandra Tanuwidjaja

Acknowledgments

This monograph was partially supported by the Institute for Information & Communications Technology Promotion (IITP) grant funded by the Korea Government (MSIT) (2013-0-00396, Research on Communication Technology using Bio-Inspired Algorithm, and 2017-0-00555, Towards Provable-secure Multi-party Authenticated Key Exchange Protocol based on Lattices in a Quantum World) and by the National Research Foundation of Korea (NRF) grant funded by the Korea Government (MSIT) (No. NRF-2015R1A-2A2A01006812).

We are very grateful for Prof. Hong-Shik Park, School of Electrical Engineering, KAIST, who gave us the excellent opportunity to execute this research initiative by combining deep learning into intrusion detection for secure wireless network. We also thank Prof. Paul D. Yoo and Prof. Taufiq Asyhari, Cranfield Defence and Security, UK, who gave us inspiring discussion during our research working.

The authors sincerely appreciate the contribution of the alumni and current member of the Cryptology and Information Security Lab. (CAISLAB), Graduate School of Information Security, School of Computing, KAIST, Khalid Huseynov, Dongsoo Lee, Kyungmin Kim, Hakju Kim, Rakyong Choi, Jeeun Lee, Soohyun Ahn, Joonjeong Park, Jeseoung Jung, Jina Hong, Sungsook Kim, Edwin Ayisi Opare, Hyeongcheol An, Seongho Han, Nakjun Choi, Nabi Lee, and Dongyeon Hong.

We gratefully acknowledge the editors of this monograph series on security for their valuable comments and the Springer to give us to write this monograph.

Finally we are also very grateful for our families for their strong support and endless love.

Contents

1	Introduction	1
	References	4
2	Intrusion Detection Systems	5
2.1	Definition	5
2.2	Classification	5
2.3	Benchmark	8
	2.3.1 Performance Metric	8
	2.3.2 Public Dataset	9
	References	10
3	Classical Machine Learning and Its Applications to IDS	13
3.1	Classification of Machine Learning	13
	3.1.1 Supervised Learning	13
	3.1.2 Unsupervised Learning	15
	3.1.3 Semi-supervised Learning	19
	3.1.4 Weakly Supervised Learning	20
	3.1.5 Reinforcement Learning	20
	3.1.6 Adversarial Machine Learning	21
3.2	Machine-Learning-Based Intrusion Detection Systems	21
	References	24
4	Deep Learning	27
4.1	Classification	27
4.2	Generative (Unsupervised Learning).....	27
	4.2.1 Stacked (Sparse) Auto-Encoder	28
	4.2.2 Boltzmann Machine	30
	4.2.3 Sum-Product Networks	30
	4.2.4 Recurrent Neural Networks	30
4.3	Discriminative	32
4.4	Hybrid	32
	4.4.1 Generative Adversarial Networks (GAN)	32
	References	33

- 5 Deep Learning-Based IDSs** 35
 - 5.1 Generative 35
 - 5.1.1 Deep Neural Network 35
 - 5.1.2 Accelerated Deep Neural Network 36
 - 5.1.3 Self-Taught Learning 37
 - 5.1.4 Stacked Denoising Auto-Encoder 38
 - 5.1.5 Long Short-Term Memory Recurrent Neural Network 38
 - 5.2 Discriminative 39
 - 5.2.1 Deep Neural Network in Software-Defined Networks 39
 - 5.2.2 Recurrent Neural Network 40
 - 5.2.3 Convolutional Neural Network 40
 - 5.2.4 Long Short-Term Memory Recurrent Neural Network 41
 - 5.3 Hybrid 42
 - 5.3.1 Adversarial Networks 42
 - 5.4 Deep Reinforcement Learning 43
 - 5.5 Comparison 43
 - References 44
- 6 Deep Feature Learning** 47
 - 6.1 Deep Feature Extraction and Selection 47
 - 6.1.1 Methodology 48
 - 6.1.2 Evaluation 52
 - 6.2 Deep Learning for Clustering 59
 - 6.2.1 Methodology 62
 - 6.2.2 Evaluation 63
 - 6.3 Comparison 65
 - References 67
- 7 Summary and Further Challenges** 69
 - References 70
- Appendix A A Survey on Malware Detection from Deep Learning** 71
 - A.1 Automatic Analysis of Malware Behavior Using Machine Learning 71
 - A.2 Deep Learning for Classification of Malware System Call Sequences 72
 - A.3 Malware Detection with Deep Neural Network Using Process Behavior 73
 - A.4 Efficient Dynamic Malware Analysis Based on Network Behavior Using Deep Learning 73
 - A.5 Automatic Malware Classification and New Malware Detection Using Machine Learning 74
 - A.6 DeepSign: Deep Learning for Automatic Malware Signature Generation and Classification 75
 - A.7 Selecting Features to Classify Malware 75

- A.8 Analysis of Machine-Learning Techniques
Used in Behavior-Based Malware Detection 76
- A.9 Malware Detection Using Machine-Learning-Based
Analysis of Virtual Memory Access Patterns 77
- A.10 Zero-Day Malware Detection 77
- References 78

Acronyms

ACA	Ant Clustering Algorithm
ACC	Ant Colony Clustering
AE	Auto-Encoder
AIS	Artificial Immune System
ANN	Artificial Neural Network
APT	Advanced Persistent Threat
ATTA-C	Adaptive Time-Dependent Transporter Ants Clustering
AWID	Aegean Wi-Fi Intrusion Dataset
BM	Boltzmann Machine
CAN	Controller Area Network
CCN	Content-Centric Network
CFS	CfsSubsetEval
CNN	Convolutional Neural Network
CoG	Center of Gravity
Corr	Correlation
CPS	Cyber-Physical System
DAE	Denoising Auto-Encoder
DBM	Deep Boltzmann Machine
DBN	Deep Belief Network
DDoS	Distributed Denial of Service
D-FES	Deep Feature Extraction and Selection
DNN	Deep Neural Network
DoS	Denial of Service
DR	Detection Rate
DT	Decision Tree
ERL	Evolutionary Reinforcement Learning
ESVDF	Enhanced Support Vector Decision Function
FIS	Fuzzy Inference System
FL	Feature Learning
FN	False Negative
FNR	False Negative Rate

FP	False Positive
FPR	False Positive Rate
FW	Firewall
GAN	Generative Adversarial Networks
GPU	Graphics Processing Unit
GRU	Gated Recurrent Unit
HJI	Hamiltonian-Jacobi-Isaac
HIS	Human Inference System
ICV	Integrity Check Value
IDS	Intrusion Detection System
IG	Information Gain
IoT	Internet of Things
IPS	Intrusion Prevention System
IV	Initialization Vector
JSON	Java Script Object Notation
KL	Kullback-Leibler
kNN	K-Nearest Neighbors
LoM	Largest of Max
LSTM	Long Short-Term Memory
MDP	Markov Decision Processes
METIS	Mobile and Wireless Communications Enablers for the Twenty-Twenty Information Society
MF	Membership Functions
MLP	Multi-Layer Perceptron
MoM	Mean of Max
MSE	Mean Square Error
NN	Neural Network
PSO	Particle Swarm Optimization
R2L	Remote to Local
RBM	Restricted Boltzmann Machine
RL	Reinforcement Learning
RNN	Recurrent Neural Networks
SAE	Stacked Auto-Encoder
SDAE	Stacked Denoising Auto-Encoder
SDN	Software-Defined Networking
SFL	Supervised Feature Learning
SGD	Stochastic Gradient Descent
SNN	Shared Nearest Neighbor
SOM	Self-Organizing Map
SoM	Smallest of Max
SPN	Sum-Product Networks
STL	Self-Taught Learning
SVM	Support Vector Machine
SVM-RFE	SVM-Recursive Feature Elimination
TBM	Time to Build Model

TCP/IP	Transmission Control Protocol/Internet Protocol
TN	True Negative
TP	True Positive
TT	Time to Test
U2R	User to Root
UFL	Unsupervised Feature Learning