

Contents

1	Introduction	1
	References	4
2	Intrusion Detection Systems	5
2.1	Definition	5
2.2	Classification	8
2.3	Benchmark	8
2.3.1	Performance Metric	9
2.3.2	Public Dataset	10
	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