	doc_1	doc_2	decision	id
cases			DUPLICATES	143

doc_1	
authors	• Rana Abou Khamis • A. Matrawy
title	Evaluation of Adversarial Training on Different Types of Neural Networks in Deep Learning-based IDSs
publication_date	2020-07-08 00:00:00
source	SupportedSources.SEMANTIC_SCHOLAR
journal	
volume	
doi	10.1109/ISNCC49221.2020.9297344
urls	• https://www.semanticscholar.org/paper/00f44fb92b02552208729e228f0f3a6e06cbdadd
id	id6943958636832344104
abstract	Network security applications, including Intrusion Detection Systems (IDS) of deep neural networks (DNN), are increasing rapidly to make detection task of anomaly activities more accurate and robust. With the rapid increase of using DNN and the volume of data traveling through systems, different growing types of adversarial attacks to defeat DNN create a severe challenge. In this paper, we focus on investigating the effectiveness of different evasion attacks and how to train a resilience deep learning-based IDS using different Neural networks, e.g., Artificial Neural Network (ANN), Convolutional Neural Networks (CNN) and Recurrent Neural Networks (RNN). We use the min-max formulation to formulate the problem of training robust intrusion detection systems against adversarial samples using two benchmark datasets. Our experiments on different deep learning algorithms and different benchmark datasets demonstrate that defense using adversarial training based min-max formulation increases the robustness of the network under the assumption of our threat model and five state-of-the-art adversarial attacks.
versions	

doc_2	
authors	• Rana Abou Khamis • Ashraf Matrawy
title	Evaluation of Adversarial Training on Different Types of Neural Networks in Deep Learning-based IDSs
publication_date	2020-07-08 23:33:30+00:00
source	SupportedSources.ARXIV
journal	None
volume	
doi	
urls	• http://arxiv.org/pdf/2007.04472v1 • http://arxiv.org/abs/2007.04472v1 • http://arxiv.org/pdf/2007.04472v1
id	id5965766274018964077
abstract	Network security applications, including intrusion detection systems of deep neural networks, are increasing rapidly to make detection task of anomaly activities more accurate and robust. With the rapid increase of using DNN and the volume of data traveling through systems, different growing types of adversarial attacks to defeat them create a severe challenge. In this paper, we focus on investigating the effectiveness of different evasion attacks and how to train a resilience deep learning-based IDS using different Neural networks, e.g., convolutional neural networks (CNN) and recurrent neural networks (RNN). We use the min-max approach to formulate the problem of training robust IDS against adversarial examples using two benchmark datasets. Our experiments on different deep learning algorithms and different benchmark datasets demonstrate that defense using an adversarial training-based min-max approach improves the robustness against the five well-known adversarial attack methods.
versions	