cases

doc_1		doc_2		decision	id
authors	• Peilun Wu • Hui Guo • Nour Moustafa	**authors**	• Peilun Wu • Hui Guo	DUPLICATES	14
title	Pelican: A Deep Residual Network for Network Intrusion Detection	**title**	Pelican: A Deep Residual Network for Network Intrusion Detection		
publication_date	2020-01-19 05:07:48+00:00	**publication_date**	2020-01-19 00:00:00		
source	SupportedSources.ARXIV	**source**	SupportedSources.SEMANTIC_SCHOLAR		
journal	None	**journal**			
volume		**volume**			
doi		**doi**	10.1109/DSN-W50199.2020.00018		
urls	• http://arxiv.org/pdf/2001.08523v7 • http://arxiv.org/abs/2001.08523v7 • http://arxiv.org/pdf/2001.08523v7	**urls**	• https://www.semanticscholar.org/paper/bfa4479631987b682696a9c8ff826e2ca588c5d4		
id	id-2176250769704850386	**id**	id-5378031934948481687		
abstract	One challenge for building a secure network communication environment is how to effectively detect and prevent malicious network behaviours. The abnormal network activities threaten users' privacy and potentially damage the function and infrastructure of the whole network. To address this problem, the network intrusion detection system (NIDS) has been used. By continuously monitoring network activities, the system can timely identify attacks and prompt counter-attack actions. NIDS has been evolving over years. The current-generation NIDS incorporates machine learning (ML) as the core technology in order to improve the detection performance on novel attacks. However, the high detection rate achieved by a traditional ML-based detection method is often accompanied by large false-alarms, which greatly affects its overall performance. In this paper, we propose a deep neural network, Pelican, that is built upon specially-designed residual blocks. We evaluated Pelican on two network traffic datasets, NSL-KDD and UNSW-NB15. Our experiments show that Pelican can achieve a high attack detection performance while keeping a much low false alarm rate when compared with a set of up-to-date machine learning based designs.	**abstract**	One challenge for building a secure network communication environment is how to effectively detect and prevent malicious network behaviours. The abnormal network activities threaten usersâ€™ privacy and potentially damage the function and infrastructure of the whole network. To address this problem, the network intrusion detection system (NIDS) has been used. By continuously monitoring network activities, the system can timely identify attacks and prompt counter-attack actions. NIDS has been evolving over years. The current-generation NIDS incorporates machine learning (ML) as the core technology in order to improve the detection performance on novel attacks. However, the high detection rate achieved by a traditional ML-based detection method is often accompanied by large false-alarms, which greatly affects its overall performance. In this paper, we propose a deep neural network, Pelican, that is built upon specially-designed residual blocks. We evaluated Pelican on two network traffic datasets, NSL-KDD and UNSW-NB15. Our experiments show that Pelican can achieve a high attack detection performance while keeping a much low false alarm rate when compared with a set of up-to-date machine learning based designs.		
versions		**versions**			