


Computing  
Reviews


**Association for  
Computing Machinery**  
  
**ThinkLoud®**

TODAY'S ISSUE
HOT TOPICS
SEARCH
BROWSE
RECOMMENDED
MY ACCOUNT
LOGIN

REVIEW
?

## Review

Search



### A deep learning technique for intrusion detection system using a recurrent neural networks based framework

Kasongo S. *Computer Communications* 199 113-125, 2023. Type: Article

Date Reviewed: Jan 19 2024



So let's assume you already know and understand that artificial intelligence's main building blocks are perceptrons, that is, mathematical models of neurons. And you know that, while a single perceptron is too limited to get "interesting" information from, very interesting structures--neural networks--can be built with them. You also understand that neural networks can be "trained" with large datasets, and you can get them to become quite efficient and accurate classifiers for data comparable to your dataset. Finally, you are interested in applying this knowledge to defensive network security, particularly in choosing the right recurrent neural network (RNN) framework to create an intrusion detection system (IDS). Are you still with me? Good! This paper might be right for you!

The paper builds on a robust and well-written introduction and related work sections to arrive at explaining in detail what characterizes a RNN, the focus of this work, among other configurations also known as neural networks, and why they are particularly suited for machine learning (ML) tasks. RNNs must be trained for each problem domain, and publicly available datasets are commonly used for such tasks. The authors present two labeled datasets representing normal and hostile network data, identified according to different criteria: NSL-KDD and UNSW-NB15. They proceed to show a framework to analyze and compare different RNNs and run them against said datasets, segmented for separate training and validation phases, compare results, and finally select the best available model for the task--measuring both training speed as well as classification accuracy.

The paper is quite heavy due to both its domain-specific terminology--many acronyms are used throughout the text--and its use of mathematical notation, both to explain specific properties of each of the RNN types and for explaining the preprocessing carried out for feature normalization and selection. This is partly what led me to start the first paragraph by assuming that we, as readers, already understand a large body of material if we are to fully follow the text. The paper does begin by explaining its core technologies, but quickly ramps up and might get too technical for nonexpert readers.

It is undeniably an interesting and valuable read, showing the state of the art in IDS and ML-assisted technologies. It does not detail any specific technology applying its findings, but we will probably find the information conveyed here soon enough in industry publications.

Reviewer: [Gunnar Wolf](#)

Review #: CR147691



Would you recommend this review?

 yes

 no

Other reviews under "Neural Nets":

Date

[Synergetic computers and cognition](#)

Oct 1 1992

Haken H. (ed), Springer-Verlag New York, Inc., New York, NY, 1991. Type: Book (9780387530307)

[Code recognition and set selection with neural networks](#)

Jun 1 1993

Jeffries C., Birkhäuser Boston Inc., Cambridge, MA, 1991. Type: Book (9780817635855)

[Fast learning and invariant object recognition](#)

Nov 1 1992

Souček B. (ed), Wiley-Interscience, New York, NY, 1992. Type: Book (9780471574309)

[more...](#)

---

 [E-Mail This](#)

 [Printer-Friendly](#)

**REVIEWER'S AREA**

**MASTHEAD**

**SUBSCRIBE**

**NEWS**

**TIPS**

**HELP**

**CONTACT US**

Reproduction in whole or in part without permission is prohibited. Copyright 1999-2024 ThinkLoud®

[Terms of Use](#) | [Privacy Policy](#)