A Review of Current Machine Learning Approaches for Anomaly Detection in Network Traffic

Wasim A. Ali [1]

Department of Computer Science and Engineering, PG Centre, Visvesvaraya Technological University, Mysore, Karnataka, India
Manasa K. N [2]

Research scholar, PET Research Center (affiliated to University of Mysore), PES College of Engineering, Mandya, Karnataka, India
Malika Bendechache [3]

Lero Research Centre, School of Computing, Dublin City University, Ireland
Mohammed Fadhel Aljunaid [4]

Department of Computer Science, Mangalore University, India
P. Sandhya [5]

Department of Computer Science and Engineering, PG Centre, Visvesvaraya Technological University, Mysore, Karnataka, India

JTDE - Vol 8, No 4 - December 2020 [6]

[7]

☆ 10 [8]

Abstract

Due to the advance in network technologies, the number of network users is growing rapidly, which leads to the generation of large network traffic data. This large network traffic data is prone to attacks and intrusions. Therefore, the network needs to be secured and protected by detecting anomalies as well as to prevent intrusions into networks. Network security has gained attention from researchers and network laboratories. In this paper, a comprehensive survey was completed to give a broad perspective of what recently has been done in the area of anomaly detection. Newly published studies in the last five years have been investigated to explore modern techniques with future opportunities. In this regard, the related literature on anomaly detection systems in network traffic has been discussed, with a variety of typical applications such as WSNs, IoT, high-performance computing, industrial control systems (ICS), and software-defined network (SDN) environments. Finally, we underlined diverse open issues to improve the detection of anomaly systems.

Please see PDF download for the full paper.
Article PDF:
307-article_text-3163-2-11-20201202.pdf [9]

Cite this article as:

Wasim A. Ali, Manasa K. N, Malika Bendechache, Mohammed Fadhel Aljunaid, P. Sandhya. 2020. *A Review of Current Machine Learning Approaches for Anomaly Detection in Network Traffic*. JTDE, Vol 8, No 4, Article 307. http://doi.org/10.18080/JTDE.v8n4.307 [11]. Published by Telecommunications Association Inc. ABN 34 732 327 053. https://telsoc.org [12]

[8] https://telsoc.org/printpdf/3061?rate=eQxnSbbvD_xh6NI1hPq_dlQZDaTa9JiAnj0M6K4GlQQ [9] https://telsoc.org/sites/default/files/journal_article/307-article_text-3163-2-11-20201202.pdf [10] https://telsoc.org/copyright [11] http://doi.org/10.18080/jtde.v8n4.307 [12] https://telsoc.org