Published on *Telsoc* (https://telsoc.org)

Denial-of-Sleep Attack Detection in NB-IoT Using Deep Learning

Tahani Bani-Yaseen [1]

Department of Electrical Engineering, School of Engineering, Princess Sumaya University for Technology, Amman, Jordan

Ashraf Tahat [2]

Department of Communications Engineering Princess Sumaya University for Technology, Amman, Jordan

Kira Kastell [3]

Office of the President, Hamm-Lippstadt University of Applied Sciences, Hamm, Germany

Talal A.Edwan [4]

Department of Computer Engineering, Faculty of Engineering, Al-Ahliyya Amman University, Amman, Jordan

Abstract

With increasing Internet-of-Things (IoT) protocols and connectivity, a growing number of attacks are emerging in the associated networks. This work presents approaches using deep learning (DL) to detect attacks in an IoT environment, particularly in narrowband Internet-of-Things (NB-IoT). By virtue of its low cost, low complexity and limited energy, an NB-IoT device will not likely permit cutting-edge security mechanisms, leaving it vulnerable to, for example, denial-of-sleep (DoSl) attacks. For performance analysis, a NB-IoT network was simulated, using ns-3, to generate a novel dataset to represent an implementation of DoSl attacks. After preprocessing, the dataset was presented to a collection of machine learning (ML) models to evaluate their performance. The considered DL recurrent neural network (RNN) models have proven capable of reliably classifying traffic, with very high accuracy, into either a DoSl attack or a normal record. The performance of a long short-term memory (LSTM) classifier has provided accuracies up to 98.99%, with a detection time of 2.54 x 10-5 second/record, surpassing performance of a gated recurrent unit (GRU). RNN DL models have superior performance in terms of accuracy of detecting DoSl attacks in NB-IoT networks, when compared with other ML algorithms, including support vector machine, Gaussian naïve-Bayes, and logistic regression.

Please refer to PDF download for the full paper.

Article PDF:
532-bani-yaseen-article-v10n3pp14-38.pdf [8]

Cite this article as:

Tahani Bani-Yaseen, Ashraf Tahat, Kira Kastell, Talal A.Edwan. 2022.*Denial-of-Sleep Attack Detection in NB-IoT Using Deep Learning*. JTDE, Vol 10, No 3, Article 532. http://doi.org/10.18080/JTDE.v10n3.532 [10]. Published by Telecommunications Association Inc. ABN 34 732 327 053. https://telsoc.org [11]

---

[1] https://telsoc.org/journal/author/tahani-bani-yaseen [2] https://telsoc.org/journal/author/ashraf-tahat [3] https://telsoc.org/journal/author/kira-kastell [4] https://telsoc.org/journal/author/talal-aedwan [5] https://telsoc.org/journal/jtde-v10-n3 [6] https://www.addtoany.com/share#url=https%3A%2F%2Ftelsoc.org%2Fjournal%2Fjtde-v10-n3%2Fa532&title=Denial-of-Sleep%20Attack%20Detection%20in%20NB-IoT%20Using%20Deep%20Learning [7] https://telsoc.org/printpdf/3728?rate=PvjjR2Ly-WcGHFCnlQJtVL2J8G8xIrLnXwVSgpme-U8 [8] https://telsoc.org/sites/default/files/journal_article/532-bani-yaseen-article-v10n3pp14-38.pdf [9] https://telsoc.org/copyright [10] http://doi.org/10.18080/jtde.v10n3.532 [11] https://telsoc.org