


Chapter 14

DDoS Attack Detection in WSN Using Modified BGRU With MFO Model

S. Venkatasubramanian

 <https://orcid.org/0000-0001-7560-0164>
Saranathan College of Engineering, India

R. Mohankumar

Saranathan College of Engineering, India

ABSTRACT

Significant challenges in the areas of energy and security persist for wireless sensor networks (WSNs). Avoiding denial-of-service assaults is a priority for safeguarding WSN networks. As open field encryption becomes the norm, conventional packet deep scan systems can no longer use open field review in layer security packets. To the existing literature evaluating the effect of deep learning algorithms on WSN lifespan, this study contributes the auto-encoder (AE) and then the bidirectional gated recurrent unit (BGRU). The learning rate of the BGRU is also chosen using the moth flame optimization technique. Learning is just one of the approaches that have emerged in response to the pressing need to distinguish between legitimate and criminal users. This chapter also demonstrated that for numerical statistical data, the sweet spot is reached when the number of records in the dataset is between three thousand and six thousand and when the percentage of overlap across categories is not less than fifty percent.

1. INTRODUCTION

An attacker can compromise a WSN's node availability by interfering with data packet transmission in a diversity of ways, including through sinkholes, wormholes, Sybils, hello floods, and (DoS) assaults (Pajila et al., 2022). DoS attacks can drain the resources of WSN nodes and cause data packet loss across the network. This research study will examine how to mitigate (DDoS) and (DoS) attacks in WSN networks with low energy requirements and high precision in attack definition (Lakshmi Narayanan et al.,

DOI: 10.4018/979-8-3693-0502-7.ch014

2021; Alsulaiman and Al-Ahmadi, 2021). In addition, service attacks starve WSN nodes by letting them take in traffic that is not intended for them. This sort of attack can happen at any tier of the WSN model scheme (Jane Nithya and Shyamala, 2022), and it causes WSN nodes to refuse network facilities to the genuine WSN nodes (Regin et al., 2023).

Intrusion detection is the strongest protection against DDoS assaults (Premkumar and Sundararajan, 2021) because of the prevalence of such attacks on WSN networks. Anomaly-based methods are the two main categories of intrusion detection (Angeline et al., 2023). Anomaly patterns need routine network connection monitoring and a comparison of current WSN network activity to historical traffic patterns (Islam et al., 2021). As a result, several strategies have been employed to enhance the effectiveness of active and passive DoS detection. Predicting and categorizing DDoS assaults is possible with the use of supervised machine learning techniques. Common techniques for this task are deep learning and K-Nearest Neighbor (KNN) (Hanif et al., 2022). In addition, the work shows that techniques are preferable to deep learning mechanisms for practical deployment since the latter requires large amounts of training data before producing accurate classification results (Belkhiri et al., 2022). This means that using the WSN network node to implement these features for use in training operations is pointless (Yuvaraj et al., 2022).

The clustering mechanism of WSN nodes and machine learning have both been presented as new methods for detecting DDoS (Abidoye and Kabaso, 2021; Yu et al., 2021). The impact of these algorithms on WSN networks has been studied in theory, but no publication has done so yet using the same simulation and dataset. In addition, due to the WSN nodes' constrained resources, any countermeasures against DDoS should be lightweight and quick. Most of the publications that surveyed the available knowledge focused on single assaults that were difficult to localize and detect in WSNs (Ismail et al., 2022; Rajest et al., 2023a). Therefore, optimum and intelligent localization methods are sought throughout the deployment of wireless sensor nodes to ensure precise node positioning and attack identification (Khan et al., 2022; Rajest et al., 2023b). The only way to fix this issue is to create a brand-new, highly efficient method. Since wireless sensor networks can be exploited in a sum of different denial-of-service (DoS) attacks (Yadav and Kumar, 2022).

In light of this, the primary influence of this study is an examination of the impact of algorithms on the WSN network dataset and an analysis of their performance in new WSN contexts. The following is a brief overview of the main results of this study:

- 1) A novel WSN network situation is presented that would help identify DoS assaults and examine the effect of this finding consumption by combining WSN nodes, attack detection using AR and MBGRU models, and the WSN dataset.
- 2) The impact of dataset size on deep learning classification performance analysis. The initial dataset was broken up into smaller and smaller chunks (in terms of record count).
- 3) Determine the impact that DoS anomaly detection performance has on the longevity of WSN networks.

The paper's remaining sections are laid out as follows. In Section 2, the survey is relevant to the efforts in DDoS assaults, machine learning, and WSN networks. Methodology, environmental progress, and policymaking are all broken down in Section 3. Section 4 indicates how to put complexity analysis in deep learning methods and the lifespan of WSN systems into practice. Section 5 provides a summary and suggestions for further research.

18 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:

www.igi-global.com/chapter/ddos-attack-detection-in-wsn-using-modified-bgru-with-mfo-model/335843

Related Content

Knowledge Graph Generation

Anjali Daisy (2020). *Neural Networks for Natural Language Processing* (pp. 115-121).

www.irma-international.org/chapter/knowledge-graph-generation/245087

Linguistic Analyzers of the Arabic Language: Linguistic Engineering Basis

Ali Boulaalamand Nisrine El Hannach (2024). *Empowering Low-Resource Languages With NLP Solutions* (pp. 25-50).

www.irma-international.org/chapter/linguistic-analyzers-of-the-arabic-language/340500

Advancements in Deep Learning for Automated Dubbing in Indian Languages

Sasithradevi A., Shoba S., Manikandan E. and Chanthini Baskar (2023). *Deep Learning Research Applications for Natural Language Processing* (pp. 157-166).

www.irma-international.org/chapter/advancements-in-deep-learning-for-automated-dubbing-in-indian-languages/314141

Advanced Applications of Generative AI and Natural Language Processing Models: Advancing Capabilities Safely in an Uncertain World

Shwetha Baliga, Harshith K. Murthy, Apoorv Sadhale and Dhruvi Upadhyaya (2024). *Advanced Applications of Generative AI and Natural Language Processing Models* (pp. 69-86).

www.irma-international.org/chapter/advanced-applications-of-generative-ai-and-natural-language-processing-models/335833

MorseEx: A Communication Application for the Deaf-Blind

Suresh Kumar Nagarajan, Geetha N., Raghav Talwar and Shivoma Ahuja (2023). *Deep Learning Research Applications for Natural Language Processing* (pp. 218-228).

www.irma-international.org/chapter/morseex/314146