A Novel Approach for Intrusion Detection in 5G Networks using Deep Learning

*Note: Sub-titles are not captured in Xplore and should not be used

1st Amit Noel Thokala
SCAI – Software Engineering (MS)
Arizona State University
Tempe, USA
athokal1@asu.edu

2nd Sai Rithvik Vaikuntam
SCAI – Software Engieering (MS)
Arizona State University
Tempe, USA
svaikunt@asu.edu

3rd Harsha Vardhan Yallavula
SCAI – Software Engineering(MS)
Arizona State University
Tempe, USA
hyallavu@asu.edu

4th Hari Priya Gottam
SCAI – Software Engineering (MS)
Arizona State University
Tempe, USA
hgottam@asu.edu

5th Vishwanath Reddy Yasa
SCAI – Software Engineering (MS)
Arizona State University
Tempe, USA
vyasa@asu.edu

6th Yashwanth Reddy Kikkuri
SCAI – Software Engineering (MS)
Arizona State University
Tempe, USA
ykikkuri@asu.edu

***Abstract*—This document is a model and instructions for LaTeX. This and the IEEEtran.cls file define the components of your paper [title, text, heads, etc.]. *CRITICAL: Do Not Use Symbols, Special Characters, Footnotes, or Math in Paper Title or Abstract.**

***Index Terms*—component, formatting, style, styling, insert**

I. Introduction

This document is a model and instructions for LaTeX. Please observe the conference page limits.

II. Problem Definition

A. Maintaining the Integrity of the Specifications

The IEEEtran class file is used to format your paper and style the text. All margins, column widths, line spaces, and text fonts are prescribed; please do not alter them. You may note peculiarities. For example, the head margin measures proportionately more than is customary. This measurement and others are deliberate, using specifications that anticipate your paper as one part of the entire proceedings, and not as an independent document. Please do not revise any of the current designations.

III. Related Work

A. An efficient deep learning model for intrusion classification and prediction in 5G and IoT networks

The paper underscores the escalating threat landscape of cyber-attacks, particularly with the pervasive use of the Internet of Things (IoT) in e-commerce, healthcare, and communication systems. As wireless network traffic is predicted to dominate Internet usage, the vulnerability of these networks becomes a critical concern, especially with the continual evolution of technologies like 5G and IoT. The literature review focuses on the burgeoning research in intrusion detection systems (IDS) and the adoption of deep learning techniques for enhanced security. The study introduces a hybrid intrusion detection system designed for low latency and high accuracy, employing an unsupervised pre-training autoencoder for feature extraction and a supervised dense neural network for classification. The evaluation, based on the Aegean Wi-Fi Intrusion Dataset (AWID), demonstrates the models effectiveness, with particular emphasis on its robust performance in detecting specific attack types. Data pre-processing, model architecture, and optimization techniques during the training phase are detailed. The authors compare their model's performance favorably against other machine learning techniques, highlighting its efficiency in feature selection. Future work is suggested to further improve detection accuracy, minimize false positives and negatives, and extend the model's applicability to a broader range of attacks, particularly in mobile and IoT security platforms. [1].

B. Wireless Intrusion and Attack Detection

Paper proposes a new system to detect cyberattacks in 5G networks, specifically focusing on "Wireless Intrusion Detection Systems" (WIDS). Machine learning, particularly deep learning, is highlighted as a potent solution due to its capacity to decipher intricate behaviors, a pivotal attribute in effective network intrusion detection. The literature extensively surveys prior research, encompassing diverse techniques such as Random Forest, Adaboost, Decision Tree, k-Nearest Neighbor, Artificial Neural Networks (ANN), Long Short-Term Memory (LSTM), and Convolutional Neural Networks (CNN). Notably, studies leveraging deep learning, including

Identify applicable funding agency here. If none, delete this.

Autoencoder, DNN, CNN, ANN, and LSTM, exhibit promising outcomes, showcasing their efficacy in achieving precise intrusion detection in the intricate 5G network landscape [2].

C. Research of Machine Learning Algorithms for the Development of Intrusion Detection Systems in 5G Mobile Networks and Beyond

This study delves into the utilization of machine learning and deep learning methodologies for network intrusion detection systems (NIDS) designed for 5G networks [3]. Employing the CIC-IDS-2017 and CSE-CIC-IDS-2018 datasets, the research unfolds across three segments. In the initial phase, the Gradient Boost algorithm demonstrates robust efficacy but grapples with issues related to misclassification in specific attack classes. The second explores unsupervised learning with autoencoder architectures, revealing limitations in achieving sufficient performance compared to traditional machine learning models. In the final phase, a supervised learning approach employing deep neural network (DNN) models attains noteworthy outcomes. However, challenges emerge in accurately distinguishing penetration attacks due to statistical resemblances between benign and penetrating traffic. The research concludes with a comparative analysis, naming the Gradient Boosted Tree model as the most effective intrusion detection in 5G networks.

D. Real-Time Intrusion Detection and Prevention System for 5G and beyond Software-Defined Networks

This paper introduces an innovative Intrusion Detection and Prevention System (IDS/IPS) leveraging a Convolutional Neural Network (CNN) model [4]. The proposed system excels in real-time processing, vital for 5G's high-speed requirements. The CNN model, employed for preprocessing and analysis, demonstrates high accuracy in identifying both known and unknown threat patterns. The architecture ensures scalability, and performance metrics, including accuracy, highlight the system's efficiency. Additionally, the paper introduces the 5G-NIDD dataset, contributing significantly to 5G network security research.

IV. Proposed Approach

A. Research of Machine Learning Algorithms for the Development of Intrusion Detection Systems in 5G Mobile Networks and Beyond

The IEEEtran class file is used to format your paper and style the text. All margins, column widths, line spaces, and text fonts are prescribed; please do not alter them. You may note peculiarities. For example, the head margin measures proportionately more than is customary. This measurement and others are deliberate, using specifications that anticipate your paper as one part of the entire proceedings, and not as an independent document. Please do not revise any of the current designations.

B. Research of Machine Learning Algorithms for the Development of Intrusion Detection Systems in 5G Mobile Networks and Beyond

The IEEEtran class file is used to format your paper and style the text. All margins, column widths, line spaces, and text fonts are prescribed; please do not alter them. You may note peculiarities. For example, the head margin measures proportionately more than is customary. This measurement and others are deliberate, using specifications that anticipate your paper as one part of the entire proceedings, and not as an independent document. Please do not revise any of the current designations. [4].

Acknowledgment

The preferred spelling of the word "acknowledgment" in America is without an "e" after the "g". Avoid the stilted expression "one of us (R. B. G.) thanks ...". Instead, try "R. B. G. thanks...". Put sponsor acknowledgments in the unnumbered footnote on the first page.

References

[1] Rezvy, S., Luo, Y., Petridis, M., Lasebae, A. and Zebin, T., 2019, March. An efficient deep learning model for intrusion classification and prediction in 5G and IoT networks. In 2019 53rd Annual Conference on information sciences and systems (CISS) (pp. 1-6). IEEE.

[2] Bayana alenazi, Dr. Hala Eldaw Idris, "Wireless Intrusion and Attack Detection for 5G Networks using Deep Learning Techniques

[3] Imanbayev, A.; Tynymbayev, S.; Odarchenko, R.; Gnatyuk, S.; Berdibayev, R.; Baikenov, A.; Kaniyeva, N. Research of Machine Learning Algorithms for the Development of Intrusion Detection Systems in 5G Mobile Networks and Beyond. Sensors 2022, 22, 9957. https://doi.org/10.3390/s22249957

[4] Bocu, R.; Iavich, M.Real-Time Intrusion Detection and Prevention System for 5G and beyond Software-Defined Networks.Symmetry 2023, 15, 110. https://doi.org/10.3390/sym15010110