Towards Detection of DDoS Attacks for Next-Gen Industrial Internet of Things

Gabriel Chukwunonso Amaizu, Cosmas Ifeanyi Nwakanma, Jae-Min Lee, and Dong-Seong Kim
Networked Systems Lab.,
IT Convergence Engineering
Kumoh National Institute of Technology
Gumi, Gyeongbuk 39177, Korea
Email: gabriel4amaizu@gmail.com, (cosmas.ifeanyi, ljmpaul, dskim)@kumoh.ac.kr

***Abstract*—In this work, we present a deep learning based Distributed Denial of Service (DDoS) detection system for next generation Industrial Internet of things (IIoT). Next generation IIoT stems from the fact that as 3GPP Release 16 is finalised on July 2020, the need to achieve massive interconnection of devices for IIOT scenario is now more urgent and critical. Massive connection of devices for the industrial scenario or IIoT is faced with security issues one of which is DDoS. The detection system developed based on deep neural network (DNN) achieved accuracy of 96%.**

***Index Terms*—DDoS, DNN, IIoT, network traffic**

I. Introduction

Internet of Things used for manufacturing or smart factory is generally considered as Industrial Internet of Things (IIoT) [1]. Distributed Denial of Service (DDoS) and Denial of Service (DoS) has been around for a while now. However, with the continuous increase in IoT device and rising application to the industry, the nature or approach of DDoS and DoS attacks are evolving and need for enhanced approach to their detection and mitigation. DDos impact the availability of data to end users as attacker can be hidden making detection of DDoS very difficult [2].

In recent time, deep learning approach to DDoS detection and mitigation is receving attention and becoming very promising [2], [3]. In [2], authors based their DDoS detection system on KDDCUP99, DAPRA and DDoS attack datsets. In [3], convolutional neural network (CNN) was adopted to mitigate DDoS attack for a 5G network. The limitations however of this two papers is that in [2] and [4], authors relied on datasets that was prevalent in 2016 but in our approach, we adopted the CICDDoS2019 [5] [6] which is an updated dataset that reflects the current and common attacks speculated to be relevant to future generation IIoT. Example of the recent DDoS attacks include but not limited to PortMap, NetBIOS, LDAP, MSSQL, UDP, UDP-Lag, SYN, NTP, DNS, and SNMP [7] [8].

In this paper, our deep learning approach achieved an accuracy of 96% which is above the 91% achived by [3]. The combined advantage of our framework based on modern DDoS attacks and accuracy makes the proposed idea a promising solution. Chiefly, the major contribution of this paper is the frame work for DDoS detection and mitigation to secure IIoT using a DNN model with five hidden layers that yields enhanced detection accuracy with reduction in computation and time complexity. Following this section I (Introduction), is Section II where we described the System model reflecting the IIoT devices that are prone to DDoS or used as Zombies to cause DDoS attacks to other IIoT devices. In Section III, we described the performance of the DNN and show its superior performance over the state-of the art. Section IV is the conclusion of the paper.

II. System Model

A. Deep Neural Network

This paper makes use of a simple DNN that consists of an input layer, five hidden layers having 32 neurons respectively and an output layer. The DNN was trained for 100 epochs and since the dataset had over 700,000 rows, we had used a batch size of 40.

B. Dataset

The CICDDoS2019 [5] [6] dataset was used in training the proposed model. The dataset consists of benign and various common DDoS attacks and was collated for two days. For simplicity purpose, we combined all DDoS attacks in the dataset and opted for a binary classification, therefore a class of 0 means no attack while 1 signifies a DDoS attack.

C. Detection Framework

We propose a model for the detection of DDoS in IIoTs as seen in Fig 1. The detection model is mounted in the base station (BS) as research has shown that it is better to secure the BS instead of individual devices for Next-Gen IIoT [9]. All network traffic is sent through the BS which has the detection model installed. When these traffics gets to the BS, the detection model checks for any DDoS attacks in real-time. If an attack is detected the system automatically flags it and drop all packest associated with it, but if the traffic is deemed as normal or benign then the system continues working as normal.

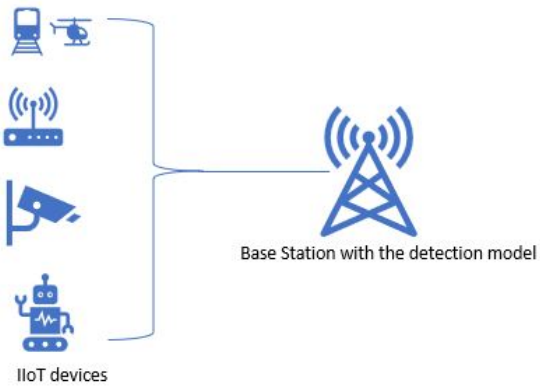

Fig. 1. System model depicting a base station servicing various IIoT devices and installed with the detection model

III. Performance Evaluation

In determining the performance of any DNN model, paper used evaluation metrics such as loss, accuracy ,recall f1-score, confusion matrix and precision, are used. Our model recorded a value of 93% for precision, 100% for recall and 96% for f1-score. Furthermore, the recorded accuracy was 96.51% and 0.064 for loss. Figs 2, 4 and 3 gives a pictorial of the confusion matrix, model accuracy and loss respectively.

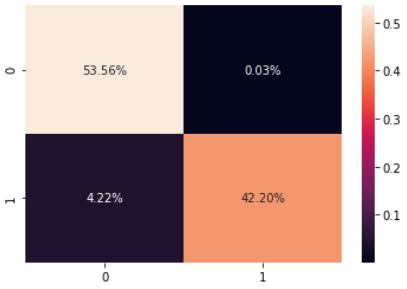

Fig. 2. Confusion matrix of proposed scheme showing

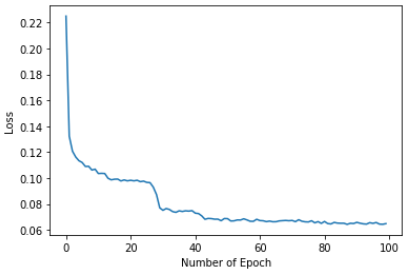

Fig. 3. Proposed scheme showing a minimal loss

IV. Conclusion

This paper implemented a DDoS attack detection for Next-Gen IIoTs using a DNN model. The model was train using CICDDoS2019 dataset which to the best of our knowledge is the latest compiled dataset for DDoS attacks. The Detection model was mounted in a BS which is responsible for disseminating traffic, and the model classifies a normal traffic as 0 and a DDoS as 1. The model recorded a high accuracy of 96% and with a low loss of 0.064 which makes the model suitable for identifying and removing DDoS attacks from a network. In no distant future, we aim to classify each individual DDoS attack and also obtain a higher detection accuracy.

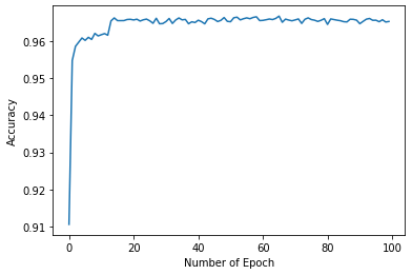

Fig. 4. Proposed scheme accuracy

Acknowledgment

This work was supported by Priority Research Centers Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology(2018R1A6A1A03024003).

References

[1] N. B. Long, H. Tran-Dang and D. Kim,"Energy-Aware Real-Time Routing for Large-Scale Industrial Internet of Things," in IEEE Internet of Things Journal, vol. 5, no. 3, pp. 2190-2199, June 2018, doi: 10.1109/JIOT.2018.2827050.

[2] R. Abubakar et al.,"An Effective Mechanism to Mitigate Real-time DDoS Attack Using Dataset," in IEEE Access, doi: 10.1109/ACCESS.2020.2995820.

[3] B. Hussain, Q. Du, B. Sun and Z. Han, "Deep Learning-Based DDoS-Attack Detection for Cyber-Physical System over 5G network," in IEEE Transactions on Industrial Informatics, doi: 10.1109/TII.2020.2974520.

[4] R. Abubakar et al., "An Effective Mechanism to Mitigate Real-time DDoS Attack Using Dataset," in IEEE Access, doi: 10.1109/ACCESS.2020.2995820.

[5] [ONLINE]: https://www.unb.ca/cic/datasets/ddos-2019.html

[6] Iman Sharafaldin, Arash Habibi Lashkari, Saqib Hakak, and Ali A. Ghorbani, "Developing Realistic Distributed Denial of Service (DDoS) Attack Dataset and Taxonomy", IEEE 53rd International Carnahan Conference on Security Technology, Chennai, India, 2019

[7] Y. Jia, F. Zhong, A. Alrawais, B. Gong and X. Cheng, "FlowGuard: An Intelligent Edge Defense Mechanism Against IoT DDoS Attacks," in IEEE Internet of Things Journal, doi: 10.1109/JIOT.2020.2993782

[8] A. Blaise, M. Bouet, V. Conan and S. Secci, "Botnet Fingerprinting: a Frequency Distributions Scheme for Lightweight Bot Detection," in IEEE Transactions on Network and Service Management, doi: 10.1109/TNSM.2020.2996502.

[9] A. Thantharate, R. Paropkari, V. Walunj, C. Beard and P. Kankariya,"Secure5G: A Deep Learning Framework Towards a Secure Network Slicing in 5G and Beyond," 2020 10th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 2020, pp. 0852-0857, doi: 10.1109/CCWC47524.2020.9031158