DeepDDoS: A Deep-Learning Model for Detecting Software Defined Healthcare IoT Networks Attacks

Avewe Bassene and Bamba Gueye

Université Cheikh Anta Diop, Dakar, Senegal
{avewe.bassene,bamba.gueye}@ucad.edu.sn

Abstract. Internet of Things (IoT) brings major security challenges that have prominent social impact. Sensors diversity as well huge amount of generated data represent a big concern for handling security issues. Therefore, companies and organizations are exposed to increasingly aggressive attacks such as ransomware, denial of service (*DoS*), and distributed denial of service (*DDoS*). Although IoT devices bring a substantial socio-economic benefits, attacks can create drastically social problems within organizations like hospitals. According to healthcare-based IoT environment, attacks can impact real-time patient data monitoring/collection and consequently effect decision making with respect to critical healthcare IoT devices such as blood pressure, blood sugar levels, oxygen, weight, and even ECGs, etc. In this paper, we propose *DeepDDoS*, a stable framework that considers deep learning techniques to detect and mitigate, in real time, DoS/DDoS attacks within healthcare-based IoT environment. By leveraging the public available CICDDoS2019 dataset, we show that *DeepDDoS* outperforms previous studies and achieves a prediction model equals to 98.8%. In addition, *DeepDDoS* architecture gives an enhanced processing delay.

Keywords: Deep Learning, Intrusion Detection System, DDoS Attacks, SDN, Healthcare Internet of Things, CICDDoS2019 dataset

1 Introduction

IoT networks are promising technologies where users, processes, data, and things are connected together via different kind of networks. For instance, medical IoT promotes real-time monitoring in order to enhance patient care. Therefore, remote advanced diagnostics can be done through telemedicine. A Healthcare-based IoT (or medical IoT) describes IoT networks and other technology gains used to monitor patient's physiological status.

Nevertheless, IoT devices are heterogeneous, and thus, they are more vulnerable to networks attacks [1] [2] [3] [4] [5]. It is worth noting that IoT networks suffer from several security issues with disastrous consequences. Health sector acts as the most targeted sector for cyber-attacks [1]. No doubt, healthcare-based IoT network devices such as blood pressure, blood sugar levels, oxygen,

weight, and even ECGs, etc. need robust security mechanisms that solely enable designated and authorized people to access to resources.

In 2018, Cisco estimated that the total number of DDoS attacks will double from 7.9 million to 15.4 million by 2023 [6]. According to an increasingly aggressive DDoS attacks, Senegal government developed cybersecurity strategies called "Digital Senegal 2025" (SN2025) [7]. The main objectives of SN2025 ("digital trust") are to guarantee necessary frameworks, tools, knowledge, resources and capacities in order to eliminate existing vulnerabilities within Senegalese information systems.

According to Healthcare-based IoT network, *DoS/DDoS* attacks target servers availability. As consequence, servers can be unreachable for a few hours to several days. Indeed, Senegalese government plans to leverage Healthcare-based IoT network in order to enhance the management of diseases such as hypertension and diabetes. For instance, 13.3% of adults are hypertensive and 41.6% do not know their status. Furthermore, blood sugar level is ignored by 84.7% of Senegalese population [7].

Indeed, understanding attacks types that are occurring are mandatory in order to mitigate their impact. To detect *DoS/DDoS* attacks types, machine learning or artificial intelligence based detection approaches have been proposed [2] [3] [4] [5]. It should be noted that machine learning techniques present several limitations [3]. In contrast, Deep Learning (DL) techniques obtain good results in many different research fields.

The paper propose three main contributions. Firstly, we provide a DL-based DoS/DDoS intrusion detection techniques suitable for healthcare IoT network that leverages Long Short Term Memory (LSTM) and Convolutional Neural Network (CNN). Secondly, we describe a dataset preprocessing mechanism that tackles the problem of socket data and missing value by avoiding overfitting. Finally, we implemented and evaluated our *DeepDDoS* proposed solution according to released CICDDoS2019 dataset and edge computing scenarios within real-time scale.

The remainder of this paper is organized as follows. Section 2 illustrates literature review. Section 3 describes our *DeepDDoS* processing architecture whereas Section 4 evaluates *DeepDDoS* performance by leveraging public CICDDoS2019 dataset. Section 5 concludes and outlines our future work.

2 Related work

In this section, we briefly discuss most recent DL mechanisms that have been used for DDoS detection attacks. In fact, [8] propose a feature extraction algorithm for maximizing CNN sensitivity to detect DDoS attacks. The obtained results show that DDoS attacks are recognized with an accuracy of 87.35%. However, none real-time detection system performance is proposed.

The authors of [2] propose *DeepDefense*, a deep learning based DDoS attack detection approach. Compared to ML algorithms, *DeepDefense* gives better performance and reduces error rate by at least 39.69%. However, the used

dataset lacks most recent attacks patterns as well as diversity. Elsayed et al. [3] propose DDoSNet, an intrusion detection system (IDS) against DDoS attacks. It combines DL techniques and RNN with an autoencoder. Similarly to [2] any implementation is proposed. Moreover, models in [3] is compared with no equivalent learning algorithms like ML, despite the limitation ML techniques as representation models [2]. Furthermore, in [4] use various ML algorithms to identify potential malicious connections.

A *CNN+LSTM* [5] model is implemented and trained to detect newly *DoS* and *DDoS* attacks types. The *CNN+LSTM* model outperforms [4] as well as other studied DL models (1d – CNN, MLP, LSTM) with an accuracy of 97.16%. However, any online test and mitigation system is proposed.

In contrast to previous works [5] [4], our *DeepDDoS* prediction model gives less processing delay and matches existing state of-the-art detection accuracy whilst ascertaining the healthcare-based IoT network security to save lives. In addition, *DeepDDoS* demonstrates consistent detection results across a range of newly sub-datasets and confirm the stability of proposed solution. To the best of our knowledge, *DeepDDoS* is the first attempt that leverages public available CICDDoS2019 dataset in order to detect real-time DDoS attack within SDN-based environments.

3 DeepDDoS proposed model

According to Healthcare-based IoT network, devices can be targeted by *DoS/DDoS* attacks in two different ways: *Standard* and *Reflection*. A large definition of these attacks is given in [9]. Since IoT servers are intended for very specific tasks [10], this paper focus on the second way of attack like *Reflection* one.

3.1 DeepDDoS architecture

Fig. 1 illustrates our proposed *DeepDDoS* framework architecture. After data processing, training and evaluation phases, the model is saved and scaled to deal with a resources-constrained device such as IoT gateway. A prediction is made based on real-time captured network traffic. Note that this online traffic can be converted to mimic the form of input that is compatible with training traffic traces. According to the prediction output ("Data Labeling" in Fig. 1), the traffic source device is either allowed to access server resources (potentially safe) or denied (header of the packet is sent through PACKET_IN message to the controller). Since the attacker can perform attacks through a different IP within the same subnet, rather than restricting the access of a single IP, we define blocking rules according to the entire subnet.

3.2 Model training and identification approach

The *DeepDDoS* prediction model has the first 1d-CNN layer with ReLU [11] activation function, which is followed by Long Short Term Memory (LSTM) layer with respect to Adam activation function.

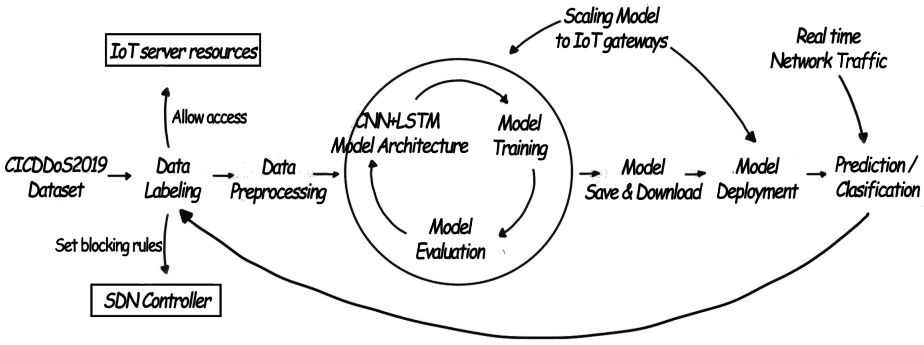

Fig. 1. DeepDDoS architecture for defining security rules on SDN controller

Since 1d-CNN accepts input shape of data in the 3D form as (batch, steps, channels), we use reshape function in *NumPy* to convert data in the following way {*data.shape(0)*, *data.shape(1)*, *1*}. Used dataset has 12 training sub-datasets. Both target variable ("Label") and no socket data are encoded using sklearn *LabelEncoder* class. The socket categorical attributes are revoked because socket information can cause overfitting. In addition, traffic attributes such as the source and destination IP addresses can be usurped [12]. The missing values are imputed using the statistics mean (*strategy*). The input shape is fedded as {83, 1}. The LSTM output from the dropout layer is connected to a fully connected layer which provides input to a dense layer with *sigmoid* function to classify attack and normal data. A dropout layer with rate 0.2 is adopted to avoid the over fitting. A batch normalisation [13] is used to accelerate the training process.

Once the model is trained, it can be used to identify potential vulnerable hosts. We save then download our training model using *model.save()*. A set of tools, *joblib* is used to dump (*joblib.dump()*) the associated data transformer. The model is loaded in a flask-script custom code at the gateway to perform prediction. This application code, with high prediction ability, aims to predict then forward any suspicious traffic through the control layer. Fig. 2 shows the overall *DeepDDoS* communication mechanism.

If a legitimate device located at, for instance at subnet 3, is attacked, generated traffic from this device would be predicted at edge as suspicious data ((1) in Fig. 2). The controller then defines the security rules (2) that aims to block the entire subnet within the same subnet IP range. Otherwise, the associated host is enabled to access to server resources (4). Since IoT devices are "predictable" thanks to generated traffic [10], any variation in its traffic can be important to take into account. Thus, we would rather get some attacked traffic labeled as attacked over leaving attacked traffic labeled not attacked.

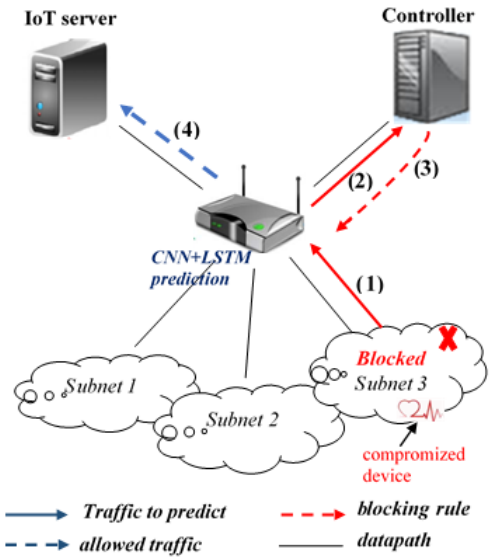

Fig. 2. A DoS/DDoS attack mitigation communication system

4 DeepDDoS performance evaluation

The performance of *DeepDDoS* prediction model is evaluated by considering standard well-known metrics such as Accuracy, Precision and Recall. The evaluation based on experimental results is done in two steps: determine proposed model efficiency in term of performance metrics and the ability to the predictor to process arrived traffic in real-time fashion.

The latest DDoS attack public CICDDoS2019 dataset [14] is considered for our extensive performance tests. The CICDDoS2019 dataset is formed by 12 DDoS attacks types categorized into 2 classes [15]. We evaluated our model by considering 10 time series. The mean performance value according to different series is selected.

Model efficiency - We measured the performance of *DeepDDoS* prediction model by classifying unseen traffic flows as benign or malicious (DDoS). Obtained results are compared to the hybrid *CNN+LSTM* model [5].

The first experiment was conducted on CICDDoS2019 sub-datasets. Fig. 3 shows that *DeepDDoS* prediction model outperforms *CNN+LSTM* proposal [5] with respect to different sub-datasets taken individually. It gives highest accuracy values between 96% (i.e. LDAP traces) to 99%. The WebDDoS traces gives the lowest accuracy value among all, near 49% (Fig. 3). Indeed, the positive class of this data is naturally be harder to detect due to the smaller number of captured samples. In fact, more WebDDoS samples are needed.

When existing sub-datasets are gathered, Table 1 gives the ability of *DeepDDoS* to obtain higher overall performance compared to *CNN+LSTM* [5]. This efficiency performance comes as an advantage of using both batch normalisation

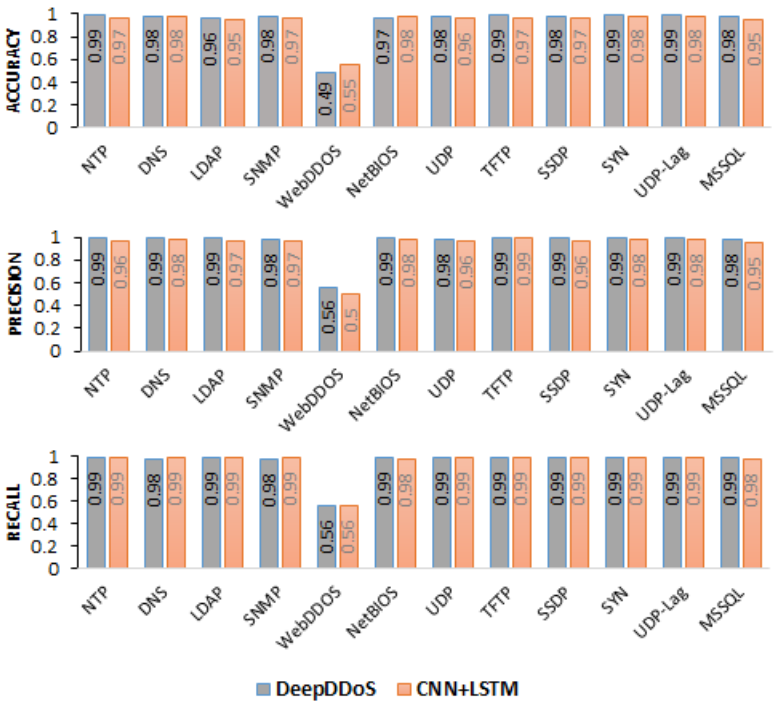

Fig. 3. Performance comparison between *DeepDDoS* and *CNN+LSTM*

and dropout layers in our model. Indeed, when training Deep Neural Networks, the distribution of each layer's inputs changes and makes it hard to train models with saturating nonlinearities.

Based on Table 1, one can see that *DeepDDoS* prediction model outperforms *CNN+LSTM* [5] approaches according to accuracy metric. Also, we observe that the performance accuracy of the well-known DL-based *CNN+LSTM* is correlated with dataset size. Indeed, the accuracy increases with the size of the dataset and it is proportional with the training time. We expect that if CICDDoS2019 raw dataset was collected within an interval of 24 hours instead of 7 hours, *DeepDDoS* will be able to achieve an accuracy upper than 98.8%. Nevertheless, *DeepDDoS* obtained precision value outperforms the hybrid *CNN+LSTM* model [5] roughly 1.59%. However, *DeepDDoS* model struggles to adapts itself from new types of attacks that have not been already classified.

Processing time - To gauge *DeepDDoS* online prediction delay, we provide an indication about the required time needed to classify several number of flows. Based on testing day traces, we randomly collected traffic flows for each application and with different sizes from 100 to 150000. This data collection process exhibits the model stability with consistent detection results across a range of sub-datasets.

Table 1. Overall accuracy comparison when merging sub-datasets

Overall Accuracy (%)				
Datasets	Unique		Merged	
Models	DeepDDoS	CNN+LSTM	DeepDDoS	CNN+LSTM
Performance	98.25	97.16	98.8	97.23

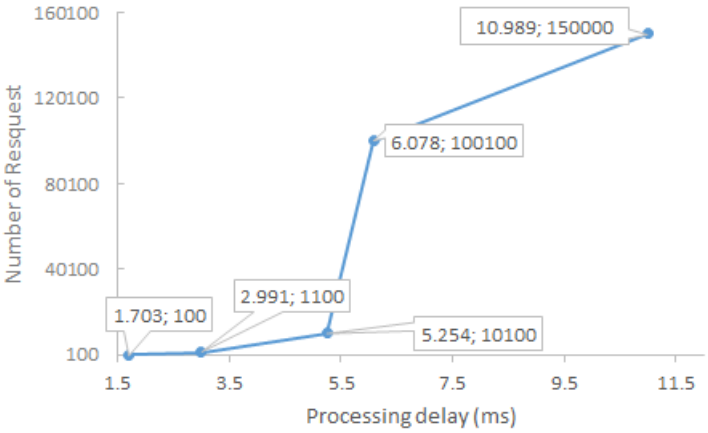

Fig. 4. Required time to classify at a glance different traffic flow requests

Fig. 4 depicts the impact of requests number with respect to prediction delay. Let t_p and t_d to be the transmission time with and without predictor, respectively. The prediction time p_t is given by Equation 1.

$$p_t = t_p - t_d \tag{1}$$

Fig. 4 illustrates that the flow processing are in correlation with respect to the number of requests. Nevertheless, whatever the number of collected requests, it can be predicted within a reasonable delay. For instance, within an interval of 10.989ms, 150000 requests are classified. The obtained time frame fits perfectly with IoT network scale transmission time.

5 Conclusion

We designed and evaluated *DeepDDoS* which an intrusion detection system that mitigates DoS/DDoS attacks within software defined healthcare IoT networks. *DeepDDoS* uses historical data in order to train an hybrid DL models. Afterwards, the obtained model is used to identify potential vulnerable IoT devices based on real-time generated traffic features. Furthermore, *DeepDDoS* embeds a SDN controller which defines security rules that aim to enable or block traffic as per the prediction output of the DL model.

DeepDDoS is evaluated using a newly comprehensive variety of DDoS attacks provided by CICDDoS2019 dataset. *DeepDDoS* prediction model outperforms the hybrid *CNN+LSTM* model [5] with an overall accuracy of 98, 8%. In contrast to previous studies, *DeepDDoS* provides a DDoS mitigation model that is able to classify up to classify 150000 requests within a interval time of 10.989ms.

As future work, we plan to simulate more WebDDoS attacks and other attacks types that can be seen according to current Internet traffic. As consequence, we will be able to address a large variety of attacks.

References

1. *https://www.vectra.ai/news/vectra-networks-identifies-healthcare-as-the-industry-most-targeted-by-cyber-attacks*, last accessed: 6-May-2020
2. X. Yuan, C. Li and X. Li: DeepDefense: Identifying DDoS Attack via Deep Learning. In Proc. SMARTCOMP, pp. 1-8, China. 2017
3. M. S. Elsayed, N. -A. Le-Khac, S. Dev and A. D. Jurcut: DDoSNet: A Deep-Learning Model for Detecting Network Attacks.IEEE 21st International Symposium on WoWMoM, pp. 391-396, Ireland, 2020
4. S. Nanda, F. Zafari, C. DeCusatis, E. Wedaa and B. Yang: Predicting network attack patterns in SDN using machine learning approach. IEEE NFV-SDN, pp. 167-172, USA, 2016.
5. M. Roopak, G. Yun Tian and J. Chambers: Deep Learning Models for Cyber Security in IoT Networks. In proc. IEEE CCWC, pp. 0452-0457, USA, 2019
6. Cisco annual internet report, *https://www.cisco.com/c/en/us/solutions/collateral-/executive-perspectives/annual-internet-report/white-paper-c11-741490.htm*, last accessed: 6-10-2020
7. *http://www.numerique.gouv.sn/sites/default/files/SNC2022-vf.pdf*, last accessed: 6-10-2020
8. M. Ghanbari and W. Kinsner: Extracting Features from Both the Input and the Output of a Convolutional Neural Network to Detect Distributed Denial of Service Attacks. IEEE ICCI*CC, USA, 2018
9. Guide to DDoS Attacks November 2017, *https://www.cisecurity.org/white-papers/technical-white-paper-guide-to-ddos-attacks*, last accessed: 06-10-2020
10. Bassene A., Gueye B.: A Group-Based IoT Devices Classification Through Network Traffic Analysis Based on Machine Learning Approach.Te-Ie-SD AFRICOMM 2020, vol 361, pp 185-202, 2021
11. R. H. Hahnloser, R. Sarpeshkar, M. A. Mahowald, R. J. Douglas, and H. S. Seung: Digital selection and analogue amplification coexist in a cortex-inspired silicon circuit. Nature, vol. 405, pp. 947–951. 2000
12. R. Doriguzzi-Corin, S. Millar, S. Scott-Hayward, J. Martínez-del-Rincón and D. Siracusa: Lucid: A Practical, Lightweight Deep Learning Solution for DDoS Attack Detection. IEEE TNSM, vol. 17, no. 2, pp. 876-889, 2020
13. S. Ioffe and C. Szegedy: Batch normalization: Accelerating deep network training by reducing internal covariate shift. 2015
14. I. Sharafaldin, A. H. Lashkari, and A. A. Ghorbani: Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization. ICISSP, pp. 108-116. Jan 2018
15. CICDDoS2019 dataset. *http://205.174.165.80/CICDataset/CICDDoS2019*, Last accessed 20-02-2021