Feature Analysis of IoT Botnet Attacks based on RNN and LSTM

Jiyeon Kim[1,3], Hyerin Won[2], Minsun Shim[2], Seungah Hong[2], Eunjung Choi[2,3]

[1]*Center for Software Educational Innovation, Seoul Women's University, Seoul, South Korea*

[2]*Dept. Of Information Security, Seoul Women's University, Seoul, South Korea*

[3]*Right AI with Security & Ethics(RAISE) Research Center, Seoul Women's University, Seoul, South Korea*

Abstract *— As the number of IoT devices rapidly increases, attacks targeting IoT devices also increase. In the IoT environment, IoT devices are vulnerable to network attacks because IoT devices are connected to the network to process collected data through the internet. In order to detect IoT attacks, developing a security solution considering characteristics of various types of IoT devices is necessary. However, it is challenging to develop a customized security solution for each type of the IoT device. Especially, traditional rule-based detection techniques would trigger massive false alarms. In this paper, we employ deep learning (DL) techniques that train empirical data. We focus on botnet attacks targeting IoT devices and develop a DL-based botnet detection system using a Recurrent Neural Network (RNN) model as well as Long Short-Term Memory (LSTM) model. As a dataset, we use N-BaIoT which is generated by injecting botnet attacks into various types of IoT devices. We train the dataset based on the DL-based system and analyse features that improve performance of the botnet detection.*

Keywords — *Internet of Things, Attacks, Botnets, N-BaIoT, Deep learning, Recurrent neural network, Long Short-Term Memory*

I. INTRODUCTION

Internet of Things (IoT) is considered as a future strategic industry and a new economic growth engine in the world. South Korea is also one of the many countries investing in IoT. South Korea invested 27.8 million U.S. dollars [1] in IoT industry over the years. However, as IoT grows, security issues on IoT are also emerging concurrently.

Numerous studies have addressed these issues in seven major ways: Object Identification and locating, Authentication and Authorization [3], Privacy, Lightweight Cryptosystems and Security protocols [4], software Vulnerability and Backdoor Analysis [5], Malware [6], and Android [2]. However, in order to detect IoT attacks, it is necessary to develop a detection model considering various types of IoT devices. Deep Learning is an effective technique to develop an attack detection model for each IoT device because it generates models by training empirical data by itself. In this paper, we focus on botnet attacks in IoT and train the N-BaIoT dataset generated by injecting Bashlite and Mirai botnet attacks into four devices such as Doorbell, Baby Monitor, Security Camera and Webcam. We develop our DL models based on RNN and LSTM models which are suitable for training time-series data. We then analyze and suggest the features of the dataset that can improve performance of botnet detection.

The remainder of this paper is as follows. We review existing Artificial Intelligence (AI) based IoT security studies in Section 2. We describe the N-BaIoT dataset and develop our DL-based model using RNN and LSTM in Section 3. We then train and test the dataset and analyze the effective features for botnet detection by IoT devices in Section 4. Finally, the conclusions are presented in Section 5.

II. RELATED WORKS

A. ML-based IoT security studies

Numerous studies employ Artificial Intelligence (AI) to detect various attacks in the traditional network environment. Although there are several widely used datasets such as KDD99 [7], NSL-KDD [8], UNSW-NB15 [9], CICIDS [10], and CSE-CIC-IDS2018 [11], these datasets are used for traditional network intrusion detection. Because these datasets are not suitable for use in detecting IoT attacks several IoT studies collects their own datasets in the IoT environment.

Janice, et al. [12] use ML in IoT gateway to help securing the system. They use ANN to monitor the system. They collect about 4,000 samples from the edge devices, and store in the MySQL database. The dataset consists of features such as device ID, sensor value, and time stamp of each data transmission. They train the dataset and show the testing accuracy of the proposed model.

Meidan et al. [13] propose a method that classifies devices by training traffic collected from both IoT devices and non-IoT devices. They employ Machine Learning (ML) models including Random Forest and Gradient Boosting Algorithm for the traffic training.

Meidan et al. [14] propose a white listing for IoT security using TCP/IP traffic data. They first deploy the white listed IoT devices such as baby monitor, motion sensor, refrigerator, security camera, smoke detector, socket, thermostat, TV and watch, and then operate the devices in a regular manner while collecting the traffic data. There are 274 features in

the originally collected dataset, and 60 features are newly added after data pre-processing.

Kotenko et al. [15] propose the framework to solve a problem of the mobile IoT security monitoring. They use the N-BaIoT dataset [22], which consists of network traffic transmitted between IoT devices. The dataset consists of 11 types of labelled samples including benign and 10 types botnet attacks belonging to Bashlite and Mirai attacks. They use several ML models such as Support Vector Machine (SVM), K-Nearest Neighbor (KNN), Gaussian Naïve Bayes (NB), and Decision Tree (DT).

TABLE I shows the summary of ML-based IoT security studies described above.

TABLE I
MACHINE LEARNING BASED DETECTION OF IOT ATTACKS

Ref.	Dataset	Model
Janice, et al. [12]	4,000 data (Device ID, Sensor value, time stamp of each data transmission) samples (Arduino Uno+ESP8266 WiFi chip + temperature sensor + Raspberry Pi to implement a gateway)	ANN
Median, et al. [13]	22,620 TCP Sessions of IoT (Baby Monitor, Motion Sensor, Printer, Refrigerator, Security Camera, Socket, Thermostat, TV. Smartwatch), 10,866 TCP Sessions of Non-IoT (PC, Laptop, Smartphone)	GBM, Random Forest, XGBoost
Median, et al. [14]	4,065,583 Client Sessions of IoT (Baby Monitor, Motion Sensor, Refrigerator, Security Camera, Smoke Detector, Socket, Thermostat, TV, Watch)	Random Forest
Kotenko , et al. [15]	detection_of_IoT_botnet_attacks_N_BaIoT - 7,009,270 instances (Doorbell, thermostat, Baby Monitor, Security Camera, Webcam)	SVM, KNN, GNB, ANN, DT, PV, WV, SV

B. DL-based IoT Security

Numerous studies have also addressed DL-based detection studies for IoT attacks.

Christopher, et al. [16] propose a detection model based on a Bidirectional LSTM based RNN (BLSTM-RNN) and compare its performance with LSTM. They propose a solution for botnet activity detection. Two Sricam AP009 IP Cameras are used as bots to attack a target (Raspberry Pi). They inject attacks such as UDP, ACK and DNS of Mirai.

B. A. Tama, et al. [17] propose a DL-based detection model using three novel benchmarking datasets for wired and wireless network environment (i.e. UNSW-NB15, CIDDS-001, and GPRS). They develop the model using Deep Neural Network (DNN). R. Das, et al. [18] propose a DL approach to an IoT authentication by using 30-node testbed of LP-WAN radios and software-radio adversaries deployed in the CMU campus. They observe that the validation accuracy increases as they increase the complexity of the LSTM.

Thamilarasu, et al. [20] propose a detection framework using both real-network traces and a simulation for providing evidence of its scalability. They use Scapy, an open source network penetration testing framework, to extract network transactions by stripping down each network packet. They simulate and evaluate the performance of their proposed framework using DNN against various attacks such as sinkhole attack and DDoS attack.

Brun. et al [21] propose a DL-based approach to the online detection of network attacks. They detect the network attacks using DNN and analyze metrics relevant to the attacks. **TABLE II** shows the summary of IoT security studies using DL.

TABLE II
DEEP LEARNING BASED DETECTION OF IOT ATTACKS

Ref.	Dataset	Model
Christopher, et al. [16]	Dataset consists of Mirai botnet and normal IP traffic (included features: number, time, source, destination, protocol, length, info)	BLSTM-RNN
B. A. Tama, et al. [17]	UNSW-NB15[9], CIDDS-001[10], GPRS[18]	DNN
R. Das, et al. [19]	Experimental validation from a 30-node testbed of LP-WAN radios and software-radio adversaries deployed in the CMU campus	LSTM
Thamilarasu, et al. [20]	dataset consists of 5 million network transactions (represented as features) from the six sensors distributed in a smart home network simulation.	DNN
Brun, et al. [21]	packets, statistical data (e.g. the rate)	DNN

III. IOT BOTNET DETECTION MODEL

A. N-BaIoT Dataset

The N-BaIoT dataset [22] was generated by injecting two types of botnet attacks such as Bashlite and Mirai. Bashlite consists of 5 types of attacks such as Scan, Junk, UDP, TCP, and COMBO, Mirai

injects Scan, ACK, SYN, UDP, and UDP Plain attacks.

N-BaIoT consists of several sub-datasets collected from various types of IoT devices such as Doorbell (Danmini, Ennio), Thermostat (Ecobee), Baby Monitor (Philips B120N/10), Security Camera (Provision PT-737E, Provision PT-838, SimpleHome XCS7-1002-WHT, SimpleHome XCS7-1003-WHT) and Webcam (Samsung SNH 1011 N).

There are a total of 115 features collected from each of the five time windows such as 100ms, 500ms, 1.5sec, 10sec and 1min. Each time window includes 23 features and the detailed explanation of the features is as follows. First, each sample with 23 features is captured with the aggregation classification as Source IP, Source MAC-IP, Channel, and Socket. First of all, in Source IP, the values of the Source IP are the packet size that is only outbound and the packet count. For each value, the corresponding statistics are mean and variance in the packet size, and integer in the packet count. The corresponding total number of features is 3. In Source MAC-IP, value and statistic appears same as the Source IP. Also, the total number of features is 3. In Channel, the values are packet size(outbound), packet count, amount of time between packet arrivals, packet size(inbound and outbound) and among the corresponding statics, packet size that is outbound and packet count are the consistent with the values in the Source IP, and others are mean, variance, and integer in the amount of time between packet arrivals, magnitude, radius, covariance, and correlation coefficient in packet size that is both inbound and outbound. The total number of features is 10. In the Socket, values are packet size(outbound), packet count, and packet size (inbound and outbound). The statistic for the three is consistent with the values in the channel, and the total number of features is 7.

B. RNN and LSTM based IoT Botnet Detection Models

RNN is a representative DL model for training time-series data. We build an RNN model to classify the dataset into 11 classes such as 10 types of attacks belonging to Bashlite and Mirai as well as benign. We use ‘softmax’ as an activation function and ‘adam’ as an adaptive learning rate optimizer.

LSTM is a model designed to overcome the Vanishing Gradient Problem that appears in RNN. Our LSTM model consists of one input layer, embedding layer and fully connected layer. The embedding layer outputs to 16 neurons, and the fully connected layer is designed to have 1 output neuron for 16 input neurons. We use ‘sigmoid’ as an activation function and ‘RMSprop’ as an adaptive learning rate optimizer.

IV. EXPERIMENTAL EVALUATION

The N-BaIoT dataset has 115 features which consist of 23 features collected for each 100ms, 500ms, 1.5sec, 10sec, and 1min time window.

In order to find out the features that are effective for IoT botnet detection performance, we divide the features to each of the time window, train the model based on the RNN and LSTM designed in Chapter 3 and compare the botnet detection accuracy.

Fig 1 shows the average performance of classifying 10 attacks and Benign that of Bashlite and Mirai based on RNN and LSTM. In all devices, accuracy of the model which is trained with features correspond to 100ms and 500ms is higher than that of 1.5sec, 10sec and 1min. In case of RNN, the features correspond to 100ms is higher than that of 500ms. And in case of LSTM, the performance of 100ms and 500ms features are similar. Among three-time windows that have low accuracy, the features which corresponds to 10sec have the best performance. But the other two showed slightly different performance superiority for each device.

TABLE III shows the attack detection accuracy based on specific attack in Security Camera which has the lowest performance in all time window. Among attack types, TCP of Bashlite was hardly detected in every time window features. UDP of Bashlite and Scan of Mirai were all detected in case of 100ms and 500ms of time window. However, in case of the other time window, the accuracy was almost 0% so it can be said that the average accuracy is lower than 100ms and 500ms features. Through the experiment, in case of IoT botnet dataset collected from N-BaIoT, the features collected every 100ms and 500ms time window present the characteristic of the botnet well so it can increase the detection accuracy.

Fig 1: Accuracy of IoT botnet detection using RNN and LSTM

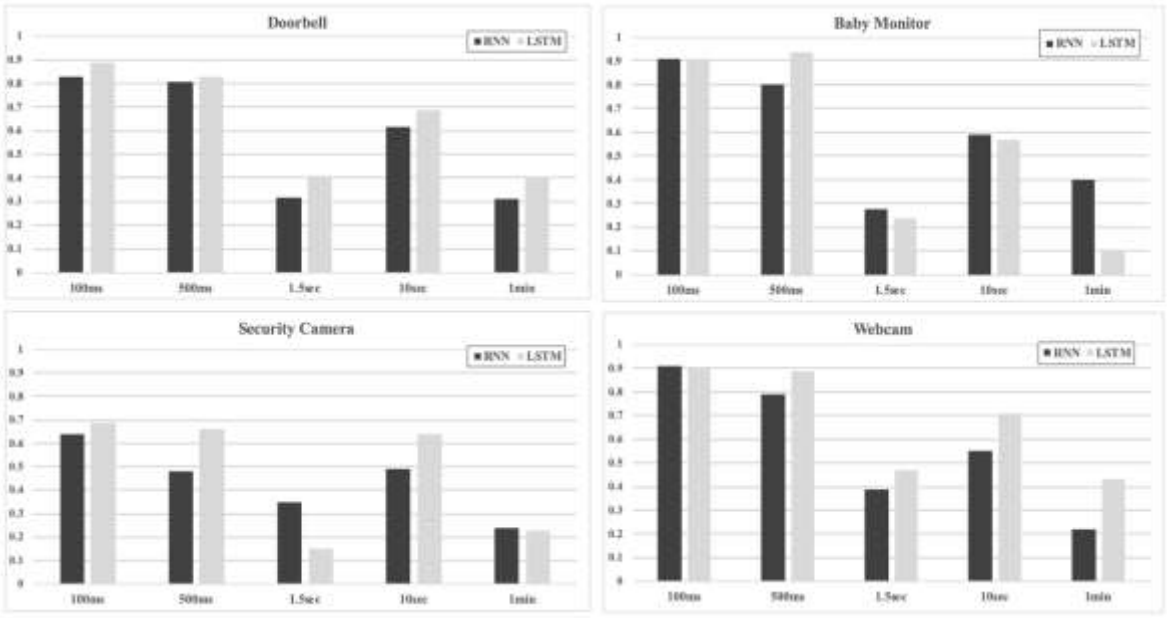

TABLE III

DETECTION ACCURACY OF IOT BOTNET ATTACKS BASED ON MULTICLASS CLASSIFICATION

Botnet	Attack	100ms		500ms		1.5sec		10sec		1min	
		RNN	LSTM	RNN	LSTM	RNN	LSTM	RNN	LSTM	RNN	LSTM
Benign		0.96	1	0.78	1	0.9	0.88	0.67	1	0.97	1
Bashlite	Combo	0.97	0.99	0.71	0.72	0.85	0.05	0.7	0.93	0.56	0.55
	Junk	0.2	0.99	0.63	0.41	0.05	0.23	0.97	0.96	0	0
	Scan	0.85	1	0.32	0.99	0.34	0.01	1	0.99	0	0
	TCP	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**
	UDP	1	1	1	1	**0**	**0**	**0**	**1**	**0**	**0**
Mirai	ACK	0.79	0.45	0.58	0.89	0.26	0.06	0.54	0.54	0.54	0.54
	Scan	1	1	0.52	1	**0**	**0**	**0**	**0**	**0**	**0**
	SYN	0.75	1	0.21	0.99	0.94	0.4	0.55	0.55	0	0
	UDP	0.56	0.03	0.52	0.25	0.2	0	0.56	0.57	0	0
	UDP Plain	0	0.05	0	0	0.33	0	0.35	0.49	0.56	0.49

V. CONCLUSIONS

In this paper, we have analyzed features of the N-BaIoT dataset for detection of botnet attacks targeting various IoT devices.

We classified 115 types of features into 5 groups considering the time window. We then train the dataset with features belonging to each time window based on RNN and LSTM models, which are used to train time-series data. In the experimental results, features with time windows of 100ms and 500ms showed the higher detection accuracy than the other features belonging to other time windows of 1.5sec, 10sec and 1min. We found out that every IoT device resulted in the similar experimental results. In other words, features collected every 100ms and 500ms not only better represent characteristics of the botnets, but can also prove that selecting these features can enhance the performance of detecting IoT botnet attacks with N-BaIoT.

ACKNOWLEDGEMENT

This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (NRF-2018R1D1A1B07050543).

REFERENCES

[1] S. Chen, H. Xu, D. Liu, B. Hu, and H. Wang, "*A vision of iot: Applications, challenges, and opportunities with china perspective*," IEEE Internet of Things journal, vol. 1, no. 4, pp. 349–359, 2014.

[2] Z. Zhang, M. Cho, C. Wang, C. Hsu, C. Chen, S. Shieh, "*IoT Security: Ongoing Challenges and Research Opportunities,"*, 2014 IEEE 7th International Conference on Service-Oriented Computing and Applications, pp. 2163-2871.

[3] J. Liu, Y. Xiao, and C. L. P. Chen, "*Authentication and Access Control in the Internet of Things,"* IEEE 32nd International Conference.

[4] Cole, Peter H., and Damith C. Ranasinghe, "*Networked RFID systems and lightweight cryptography*," Springer, 2008.

[5] A. Cui and S. J. Stolfo, "*Reflections on the engineering and operation of a large-scale embedded device vulnerability scanner,"* BADGERS, 2011.

[6] X. Xu, "*Study on Security Problems and Key Technologies of the Internet of Things*," Computational and Information Sciences (ICCIS), 2013 Fifth International Conference, pp.407,410, 21-23, 2013.

[7] S. Hettich and S. Bay, "*KDD Cup 1999 Data - The UCI KDD Archive. Irvine, CA: University of California, Department of Information and Computer Science*." 1999. [Online]. Available: http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html

[8] "*NSL-KDD | Datasets | Research | Canadian Institute for Cybersecurity | UNB*," 2016. [Online]. Available: http://www.unb.ca/cic/research/datasets/nsl.html

[9] N. Moustafa and J. Slay, "*UNSW-NB15: a comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set)*," in 2015 Military Communications and Information Systems Conference (MilCIS), Nov. 2015, pp. 1–6.

[10] C. I. for Cybersecurity (CIC), "*IDS 2017 | Datasets | Research | Canadian Institute for Cybersecurity | UNB*," 2017. [Online]. Available: https://www.unb.ca/cic/datasets/ids-2017.html

[11] "*CSE-CIC-IDS2018 | Datasets | Research | Canadian Institute for Cybersecurity | UNB*," 2018. [Online]. Available: https://www.unb.ca/cic/datasets/ids-2018.html

[12] J, Cañedo, A. Skjellum, "*Using machine learning to secure IoT systems,"* 2016 14th Annual Conference on Privacy, Security and Trust (PST), 2016.

[13] Y. Meidan, M. Bohadana, A. shabtai, "*ProfilIoT: A Machine Learning Approach for IoT Device Identification Based on Network Traffic Analysis,"* SAC '17: Proceedings of the Symposium on Applied Computing, pp. 506-509, 2017.

[14] Y. Meidan, M. Bohadana, A. shabtai, "*Detection of Unauthorized IoT Devices Using Machine Learning Techniques*," arXiv, 2017.

[15] IV Kotenko, I Saenko, A Branitskiy, "*Applying Big Data Processing and Machine Learning Methods for Mobile Internet of Things Security Monitoring*," Internet Serv. Inf. Secur., 2018.

[16] C. D. McDermott, F. Majdani, A. V. Petrovski, "*Botnet Detection in the Internet of Things using Deep Learning Approaches,"* International Joint Conference on Neural Networks (IJCNN), 2018.

[17] B. A. Tama, K. Rhee, *"Attack Classification Analysis of IoT Network via Deep learning Approach,",* 2018.

[18] D. W. Vilela, T. F. Ed'Wilson, A. A. Shinoda, N. V. de Souza Araujo, R. de Oliveira, and V. E. Nascimento. A dataset for evaluating intrusion detection systems in IEEE 802.11 wireless networks. In Proc. of the 2014 IEEE Colombian Conference on Communications and Computing (COLCOM'14), Bogota, Colombia, pages 1–5. IEEE, 2014.

[19] R. Das, A. Gardre, S. Zhang, S. Kumar, J. M. F. Moura, "*A Deep Learning Approach to IoT Authentication*," 2018 IEEE International Conference on Communications (ICC), 2018.

[20] C. Thamilarasu, S. Chawla, "*Towards Deep-Learning-Driven Intrusion Detection for the Internet of Things*," 2019.

[21] O. Brun, Y. Yin, J. Augusto, M. Ramos, E. Celenbe, "*IoT Attack Detection with Deep Learning*", 2019.

[22] MEIDAN, Yair, et al. N-baiot—network-based detection of iot botnet attacks using deep autoencoders. IEEE Pervasive Computing, 2018, 17.3: 12-22.