ISSN 1816-6075 (Print), 1818-0523 (Online)
Journal of System and Management Sciences
Vol.12 (2022) No.1, pp.44-52
DOI:10.33168/JSMS.2022.0104

Behavior Detection Mechanism for Trust Sensor Data Using Deep Learning in IoT

Hyun-Woo Kim [1] and Eun-Ha Song [2]

[1] Baewha Women's University, Seoul, Republic of Korea

[2] Wonkwang University, Iksan, Jeonbuk, Republic of Korea

ehsong@wku.ac.kr

Abstract. In this paper, we propose BDM-TSD (Behavior Detection Mechanism for Trust Sensing Data) to classify risk group and non-risk group for reliable sensor data identification in IoT environment with sensing function. BDM-TSD collects trust data such as sensing time, operation cycle, and type of sensing data of sensor devices connected to the IoT environment and artificial malicious data. The collected data performs network packet analysis and sensing data behavior analysis through the behavior of the sensor device that is subsequently operated through deep learning. Previously, research was conducted to detect unauthorized system calls of each device through security agents or abnormal behaviors through monitoring servers, and research to detect new and variant malicious behaviors with advanced attack techniques in IoT environments is insufficient A trusted IoT configuration is possible through malicious packet filtering and multi-sensor behavior detection. In this paper, we show how deep learning can be used to detect anomalies and malicious behaviors in the IoT environment based on the sensing function of multiple sensors.

Keywords: Deep Learning, Internet of Things, Behavior Detection Mechanism, Anomaly Detection, Secure Internetwork.

1. Introduction

Recently, according to the rapid development of the IT field, the quality of life has been greatly improved through various automation services using miniaturized devices. The miniaturized device includes a mobile device that can move and a fixed static device, and the Internet of Things environment is configured with these devices (Byun S, 2020; Siddiqui, 2020; Kim HW, 2021). There are various types of devices, from devices equipped with only simple sensing functions to devices with various sensing functions and capable of computing processing. Through this, it is affecting various fields such as smart cities, unmanned factories, autonomous vehicles and energy, medical, manufacturing, finance, building/housing, and customer service (Khraisatl A, 2019; Khanam S, 2020; Wang X, 2018). In the Internet of Things (IoT) environment, numerous data are collected and transmitted through various sensing devices. In the IoT environment, a lot of research is being conducted because the types of devices used for each service field are diverse and standardized architectures or security guidelines are not clearly applied (Mahdavinejad MS, 2018). In addition, it is being developed to perform an operation with a small overhead due to a small battery capacity, which is a disadvantage of a miniaturized device, and it is difficult to apply a high-level security application for service maintenance (Park H, 2021; Lydia EL, 2021).

In the IoT environment, various attacks such as denial of service (DoS) attack, botnet attack, spoofing attack, mirai attack, worm attack, packet sniffing attack, replay attack, and fuzzy attack exist (Siddiqui ST, 2020; Khanam S, 2020). In order to block new malicious behaviors and attacks from these security threats, we are conducting supervised and unsupervised learning with deep learning-based malicious behavior characteristics and normal and abnormal behavior patterns. We are researching and developing a security agent with a function to classify suspected malicious behavior based on the learned results (Yavuz FY, 2018; Parra GDLT, 2020; Diro AA, 2017; Wu D, 2019).

Furkan Yusuf Yavuz (Yavuz FY, 2018) proposed a deep learning-based routing attack detection method to effectively defend against network layer attacks that are vulnerable due to the limited resources of IoT devices in the Internet of Things environment. As a routing attack, hello-flood attack, decreased rank attack, version number attack, etc. were successfully detected, but it is difficult to respond to the new attack type due to the difficulty in data set creation. In addition, since it is difficult to identify the tampering of the sensed data, it is impossible to determine whether the data is reliable data. In this paper, it is possible to detect new behaviors because the types of normal behavior criteria are identified.

Gonzalo De La Torre Parra (Parra GDLT, 2020) proposed a cloud-based distributed deep learning framework. This framework constructs a distributed convolutional neural network model for detecting phishing and distributed dos (DDoS) attacks in the application layer, and a cloud-based temporal Long-Short

Term Memory (LSTM) network model for detecting botnet attacks. The proposed model detected more than 90% of phishing attacks and botnet attacks. Although it showed high accuracy for the attack, it is difficult to apply to detect new malicious behaviors.

Abebe Abeshu Diro (Diro AA, 2017) proposed a deep learning-based IoT and fog network attack detection system. He showed the result of detecting cyberattacks better than the centralized algorithm through measures such as accuracy, detection rate, and false alarm rate in the Internet of Things environment trained using the NSL-KDD data set.

Dapeng Wu (Wu D, 2019) proposed a new feature-based learning system for IoT applications to effectively classify sensing data generated in the IoT and detect anomalies. Although security aspects are not considered, computational overhead and energy consumption can be reduced if applied between peer data transmissions.

In this paper, we propose a behavior detection mechanism for trust sensing data (BDM-TSD) that identifies malicious packet filtering and multi-sensor behavior detection through deep learning considering the low specifications of IoT devices. BDM-TSD is capable of anomaly detection and malicious behavior detection in an IoT environment.

2. BDM-TSD Scheme

BDM-TSD analyzes transmitted and received packet information for transmission of sensing data and information sharing between IoT devices. Afterwards, it trains the Long Short Term Memory (LSTM) model and determines malicious behavior by detecting abnormalities in the generated network packets and sensing data. Since command codes can be inserted into the sensed data, WireShark, a packet analysis tool, analyzes general sensed data, system calls, and opcodes, and creates log files. Figure 1 shows the flow of BDM-TSM, and the training set consists of malicious behavior and information about process focus and sensing data routing. Usage Analyzer analyzes CPU usage, memory usage, network usage, and battery usage for operation events in IoT devices. In addition, the value of the sensed data is logged based on time series. Behavior Analyzer analyzes the behavior of known background system processes. In addition, the existing abnormal behavior is analyzed. Features are extracted through Usage Analyzer and Behavior Analyzer. Extraction includes call sequence and frequency of network packets. The extracted data is word-embedded through a one-hot encoding technique. Through this, it is possible to detect malicious behavior of packets and abnormalities in sensing data in BDM-TSD.

Malicious packet filtering of BDM-TSD is applied through network packet capture, packet data pre-processing, and learning. Table 1 shows the related network packet metadata for malicious packet filtering.

Table 2 shows the metadata used to secure the reliability of the sensor data of

BDM-TSD. SID, S-TYPE, S-DATA, TB, CB, S-Cycle, and STATUS information are used as common functions for each sensor.

Behavior capture for application to BDM-TSD uses Wireshark to analyze packets. Using the filtering function, it is classified into a packet for transmitting sensing data, a packet for maintaining the network topology, and an attack packet. For feature filtering for behavior detection, features are selected according to the packet call sequence and frequency of malicious behavior. In addition, it is possible to determine the malicious behavior and the normal behavior by selecting the normal characteristics of the packet for transmitting the sensing data.

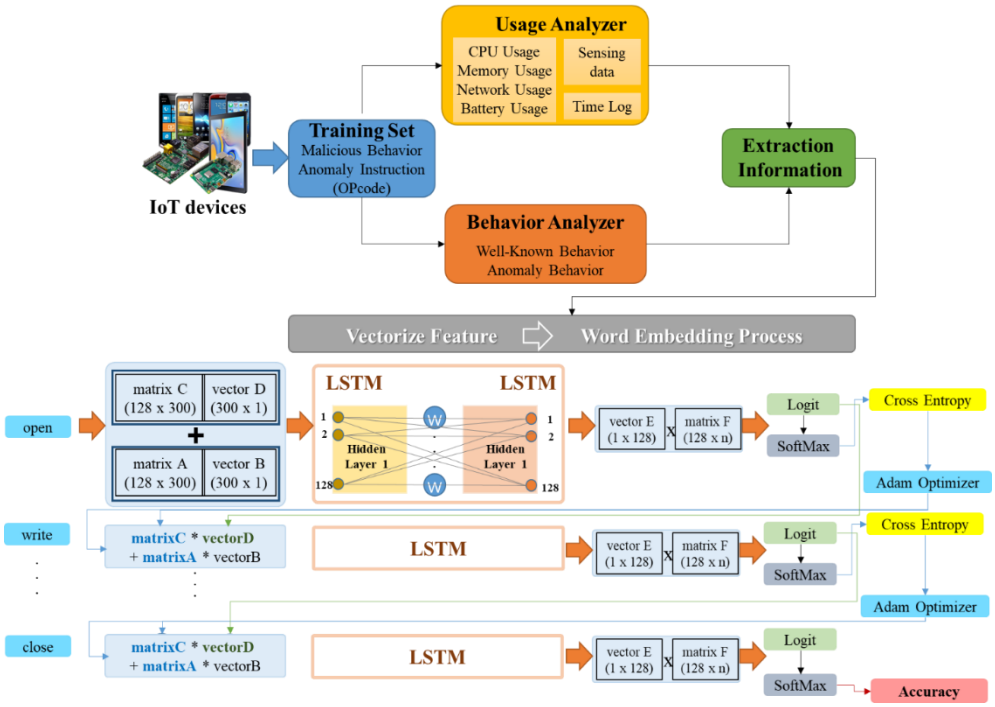

Fig. 1: Overview of BDM-TSD

Table 1: malicious behaviour metadata

Type	**Description**
PID	Process ID running on IoT device
TTL(Time to Live)	The validity period of the packet
Header Length	It means the length of the header and consists of at least 20 bytes
Header Checksum	Used to detect errors in transmitted packets
Source IP Address	IP address participating in the network, meaning the packet's

	source address
Destination IP Address	IP address participating in the network, which means the destination address of the packet
Source Port	Source port number for data transmission
Destination Port	The port number of the destination for data transmission
Protocol	Protocol for data transmission in networks
Data	Means the data being transmitted and contains sensed data or heartbeat
Total Length	The size of the packet including header and data

Table 2: configure of sensing data over BDM-TSD

Type	**Description**
SID	The identification number of the IoT device, which means sensor id
S-TYPE	The type of sensor
S-DATA	Sensed data, meaning a string-type value
TB (Total Battery)	Total battery capacity of device in IoT environment configured based on BDM-TSD
CB (Current Battery)	Remaining battery capacity of device in IoT environment configured based on BDM-TSD
S-Cycle	The sensing cycle
STATUS	Operation mode of the sensor (operation status such as waiting, executing, complete, error, etc.)

Behavioral data preprocessing is divided into extract data integration and data embedding. Extracted data integration processes continuously collected data such as opcodes of datasets, system calls, packets for transmitting sensing data, and attack packets as embedding vectors. For embedding vector, word embedding using one-hot encoding technique.

The input gate of the LSTM determines how much information at the current time is reflected in the cell and calculates the information. The output gate determines the amount to be output as the current hidden layer value, and when the difference vector between the predicted value and the actual value is obtained, the error vector is fitted to the multivariate Gaussian distribution using the maximum likelihood method. Likelihood detects abnormal behavior through the difference from the center distance of the multivariate Gaussian distribution. By learning these

features, malicious behavior is identified.

In order to secure the reliability of the sensing data, the sensing data transmission packet is learned. In BSD-TSD, the first malicious behaviour detection and the second trust data verification are performed through two learning models.

3. Implementation and Performance Evaluation of BDM-TSD

The IoT device used to build the BDM-TSD proposed in this paper was equipped with an OS function and a sensing function. In addition, for LSTM learning, it was conducted in the environment of AMD FX-8370E CPU and 24.6GB of available memory. In order to detect IoT malicious behavior, the malicious code data set and artificial attack data disclosed at BIG 2015 of the Microsoft Malware Classification Challenge were created. For the attack data, hping3, an attack tool installed by default in the terminal where Kali Linux is installed, was used. The behavioral capture of BDM-TSD captures packets generated by connected IoT devices and classifies them into packets for transmitting sensing data, packets for maintaining network topology, and attack packets. The extracted data was trained on the LSTM model using the Tensorflow library. The packet for maintaining the network topology means heartbeat, which is a survival signal between each other. In this packet, a lot of data is generated and piled up over time, and only the connection address is different in the same format. Therefore, duplicate packets are not processed in filtering for efficiency of operation, and duplicate packets are removed. The packet for sensing data transmission was learned including the SID because the data size and transmission period are different for each sensor function. This is a case where there is a fixed sensing function for each SID, and it is labeled to detect when unnecessary operation requests or sensing data that cannot be collected are transmitted. The data collected in Figure 2 is converted into an embedding vector value and used as input data of the LSTM.

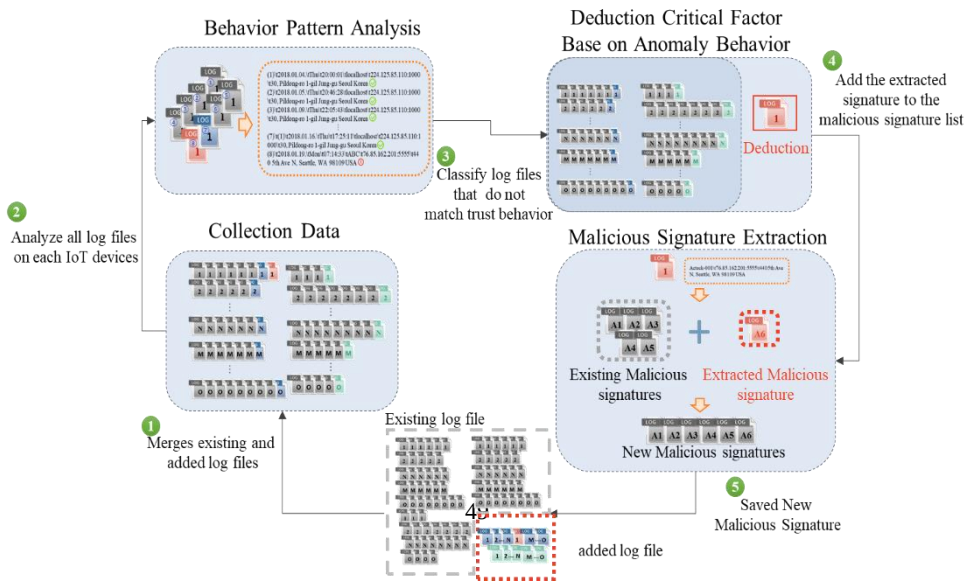

Fig. 2: Behavior Analysis and Malicious Signature Extraction of BDM-TSD

When the epoch was set to 100 to evaluate the performance of BDM-TSD, the learning accuracy was 97.71%, the loss value was 0.215, and the learning accuracy was 97.43% when other test data were used. Table 3 is set by increasing the number of cells to determine the accuracy of BDM-TSD. At this time, the number of cells was set in three types, such as 64, 128, and 256. The number of cells can be up to 256 due to hardware performance restrictions of the built BDM-TSD. In addition to the malicious behaviour data provided in BIG 2015, attacks with little training data or poorly detected attacks were oversampled to increase the rate. Basically, attacks that do not differ significantly in characteristics from normal packets were not detected. Looking at the results in Table 3, it can be seen that there is no significant difference between the accuracy of 128 cells and 256 cells. However, looking at the false positive rate (FPR) and false negative rate (FNR), it can be seen that in the case of cell 128, it is low to detect a normal packet abnormally or to determine a malicious behaviour packet as normal.

Table 3: Test accuracy of BDM-TSD with increasing cell count

Cell	Hidden Layer	Test accuracy (%)	FPR (%)	FNR (%)
64	2	98.71	4.08	0.9
128	2	99.51	0.45	0.52
256	2	99.53	0.51	0.57

Table 4 shows the results when looking at the case of 128 cells in Table 3 and setting the number of hidden layers differently. Due to the hardware specifications of the built BDM-TSD, up to three hidden layers were set. As a result, when two hidden layers were applied, the accuracy was 99.51% and the FNR was low.

Table 4: Test accuracy of BDM-TSD with increasing cell count

Cell	Hidden Layer	Test accuracy (%)	FPR (%)	FNR (%)
128	2	99.51	0.45	0.52
128	3	99.47	0.41	0.62

4. Conclusion

In this paper, we propose a BDM-TSD for detecting anomalies based on deep learning to secure reliable sensing data in the IoT environment. BDM-TSD enables active and efficient detection of malicious behaviors when short-term reliability is

important or when wired voltage is connected through learning of network attack packets and sensing data packets. However, if a request is made in the form of a security agent rather than a packet sniffing method to determine whether there is an abnormality in every packet, there is a possibility that the battery consumption due to two sensing data transmissions may be fast. For this purpose, an IoT device acting as a relay node or sink node needs to be connected to a wired voltage. In the future, we plan to conduct research for minimizing overhead between transmissions, real-time learning, and detecting anomalies.

Acknowledgements

This paper was supported by Wonkwang University in 2021.

References

Byun S. (2020). Stability-Aware Clustered Replication Scheme for IoT Data. *Journal of Next-generation Convergence Technology Association*, 4(5), 444-452.

Diro AA, Chilamkurti N. (2017). Distributed attack detection scheme using deep learning approach for Internet of Things. *Future Generation Computer Systems*, 82. 761-768.

Khanam S, Ahmedy IB, Idris MYI, Jaward MH, Sabri AQBM. (2020). A Survey of Security Challenges. *Attacks Taxonomy and Advanced Countermeasures in the Internet of Things*, 8, 219709-219743.

Khraisat A, Gondal I, Vamplew P, Kamruzzaman J, Alazab A. (2019). A Novel Ensemble of Hybrid Intrusion Detection System for Detection Internet of Things Attacks. *Electronics*, 8(11), 1-18.

Kim HW, Song EH. (2021). Deep Packet Filtering Mechanism for Secure Internetwork. *Turkish Journal of Computer and Mathematics Education*, 12(6), 502-507.

Lydia EL, Jovith AA, Devaraj AFS, Seo CH, Joshi GP. (2021). Green Energy Efficient Routing with Deep Learning Based Anomaly Detection for Internet of Things (IoT) Communications. *Mathematics*, 9(5), 1-18.

Mahdavinejad MS, Rezan M, Barekatain M, Adibi P, Barnaghi P, Sheth AP. (2018). Machine Learning for internet of things data analysis: a survey. *Digital Communications and Networks*, 4(3), 161-175.

Park H, Park DH, Kim SH. (2021). Anomaly Detection of Operating Equipment in Livestock Farms Using Deep Learning Techniques. *Electronics*, 10(16), 1-22.

Parra GDLT, Rad P, Choo KKR, Beebe N. (2020). Beebe N. Detecting Internet of Things attacks using distributed deep learning. *Journal of Network and Computer Applications*, 163(1), 102662.

Siddiqui ST, Alam S, Ahmad R, Shuaib M. (2020). Security Threats, Attacks, and Possible Countermeasures in Internet of Things. *Advances in Data and Information Sciences*, 94, 35-46.

Wang X, Wang X, Mao S. (2018). RF Sensing in the Internet of Things: A General Deep Learning Framework. *IEEE Communications Magazine*, 56(9), 62-67.

Wu D, Shi H, Wang H, Wang R, Fang H. (2019). A Feature-Based Learning System for Internet of Things Applications. *IEEE Internet of Things Journal*. 6(2), 1928-1937.

Yavuz FY, Ünal D, Gül, E. (2018). Deep Learning for Detection of Routing Attacks in the Internet of Things. *International Journal of Computational Intelligence Systems*, 12(1), 39-58.