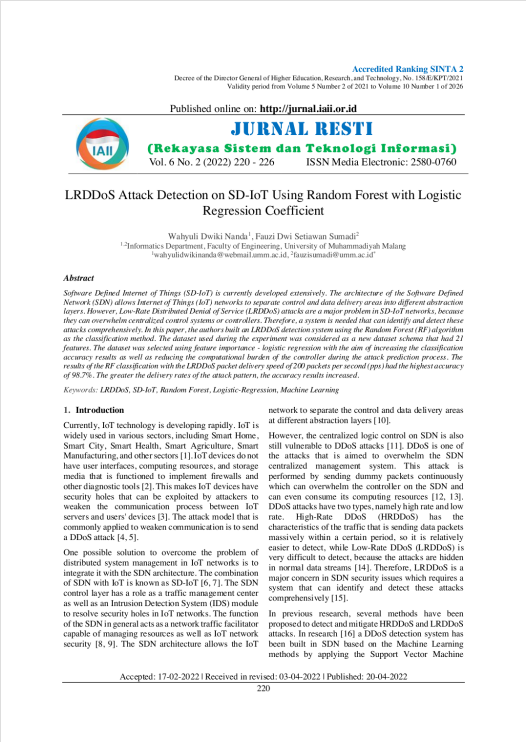
Digital Receipt

This receipt acknowledges that Turnitin received your paper. Below you will find the receipt information regarding your submission.

The first page of your submissions is displayed below.

Submission author:	Sumadi Fauzi
Assignment title:	Penelitian Dosen
Submission title:	LRDDoS Attack Detection on SD-IoT Using Random Forest wit...
File name:	Kepangkatan_Fauzi_B9.pdf
File size:	288.08K
Page count:	7
Word count:	5,171
Character count:	27,730
Submission date:	19-Jul-2023 08:48PM (UTC+0700)
Submission ID:	2133565379



Accredited Ranking SINTA 2
Decree of the Director General of Higher Education, Research, and Technology, No. 158/E/KPT/2021
Validity period from Volume 5 Number 2 of 2021 to Volume 10 Number 1 of 2026

Published online on: http://jurnal.iaii.or.id

JURNAL RESTI
(Rekayasa Sistem dan Teknologi Informasi)
Vol. 6 No. 2 (2022) 220 - 226 ISSN Media Electronic: 2580-0760

LRDDoS Attack Detection on SD-IoT Using Random Forest with Logistic Regression Coefficient

Wahyuli Dwiki Nanda[1], Fauzi Dwi Setiawan Sumadi[2]
[1,2]Informatics Department, Faculty of Engineering, University of Muhammadiyah Malang
[1]wahyulidwikinanda@webmail.umm.ac.id, [2]fauzisumadi@umm.ac.id*

Abstract

Software Defined Internet of Things (SD-IoT) is currently developed extensively. The architecture of the Software Defined Network (SDN) allows Internet of Things (IoT) networks to separate control and data delivery areas into different abstraction layers. However, Low-Rate Distributed Denial of Service (LRDDoS) attacks are a major problem in SD-IoT networks, because they can overwhelm centralized control systems or controllers. Therefore, a system is needed that can identify and detect these attacks comprehensively. In this paper, the authors built an LRDDoS detection system using the Random Forest (RF) algorithm as the classification method. The dataset used during the experiment was considered as a new dataset schema that had 21 features. The dataset was selected using feature importance - logistic regression with the aim of increasing the classification accuracy results as well as reducing the computational burden of the controller during the attack prediction process. The results of the RF classification with the LRDDoS packet delivery speed of 200 packets per second (pps) had the highest accuracy of 98.7%. The greater the delivery rates of the attack pattern, the accuracy results increased.

Keywords: LRDDoS, SD-IoT, Random Forest, Logistic-Regression, Machine Learning

1. Introduction

Currently, IoT technology is developing rapidly. IoT is widely used in various sectors, including Smart Home, Smart City, Smart Health, Smart Agriculture, Smart Manufacturing, and other sectors [1].IoT devices do not have user interfaces, computing resources, and storage media that is functioned to implement firewalls and other diagnostic tools [2]. This makes IoT devices have security holes that can be exploited by attackers to weaken the communication process between IoT servers and users' devices [3]. The attack model that is commonly applied to weaken communication is to send a DDoS attack [4, 5].

One possible solution to overcome the problem of distributed system management in IoT networks is to integrate it with the SDN architecture. The combination of SDN with IoT is known as SD-IoT [6, 7]. The SDN control layer has a role as a traffic management center as well as an Intrusion Detection System (IDS) module to resolve security holes in IoT networks. The function of the SDN in general acts as a network traffic facilitator capable of managing resources as well as IoT network security [8, 9]. The SDN architecture allows the IoT network to separate the control and data delivery areas at different abstraction layers [10].

However, the centralized logic control on SDN is also still vulnerable to DDoS attacks [11]. DDoS is one of the attacks that is aimed to overwhelm the SDN centralized management system. This attack is performed by sending dummy packets continuously which can overwhelm the controller on the SDN and can even consume its computing resources [12, 13]. DDoS attacks have two types, namely high rate and low rate. High-Rate DDoS (HRDDoS) has the characteristics of the traffic that is sending data packets massively within a certain period, so it is relatively easier to detect, while Low-Rate DDoS (LRDDoS) is very difficult to detect, because the attacks are hidden in normal data streams [14]. Therefore, LRDDoS is a major concern in SDN security issues which requires a system that can identify and detect these attacks comprehensively [15].

In previous research, several methods have been proposed to detect and mitigate HRDDoS and LRDDoS attacks. In research [16] a DDoS detection system has been built in SDN based on the Machine Learning methods by applying the Support Vector Machine

Accepted: 17-02-2022 | Received in revised: 03-04-2022 | Published: 20-04-2022

LRDDoS Attack Detection on SD-IoT Using Random Forest with Logistic Regression Coefficient

by Sumadi Fauzi

Submission date: 19-Jul-2023 08:48PM (UTC+0700)
Submission ID: 2133565379
File name: Kepangkatan_Fauzi_B9.pdf (288.08K)
Word count: 5171
Character count: 27730

Accredited Ranking SINTA 2
Decree of the Director General of Higher Education, Research, and Technology, No. 158/E/KPT/2021
Validity period from Volume 5 Number 2 of 2021 to Volume 10 Number 1 of 2026

Published online on: **http://jurnal.iaii.or.id**

JURNAL RESTI
(Rekayasa Sistem dan Teknologi Informasi)
Vol. 6 No. 2 (2022) 220 - 226 ISSN Media Electronic: 2580-0760

LRDDoS Attack Detection on SD-IoT Using Random Forest with Logistic Regression Coefficient

Wahyuli Dwiki Nan, Fauzi Dwi Setiawan Sumadi[2]
[1,2]Informatics Department, Faculty of Engineering, University of Muhammadiyah Malang
[1]wahyulidwikinanda@webmail.umm.ac.id, [2]fauzisumadi@umm.ac.id*

Abstract

Software Defined Internet of Things (SD-IoT) is currently developed extensively. The architecture of the Software Defined Network (SDN) allows Internet of Things (IoT) networks to separate control and data delivery areas into different abstraction layers. However, Low-Rate Distributed Denial of Service (LRDDoS) attacks are a major problem in SD-IoT networks, because they can overwhelm centralized control systems or controllers. Therefore, a system is needed that can identify and detect these attacks comprehensively. In this paper, the authors built an LRDDoS detection system using the Random Forest (RF) algorithm as the classification method. The dataset used during the experiment was considered as a new dataset schema that had 21 features. The dataset was selected using feature importance - logistic regression with the aim of increasing the classification accuracy results as well as reducing the computational burden of the controller during the attack prediction process. The results of the RF classification with the LRDDoS packet delivery speed of 200 packets per second (pps) had the highest accuracy of 98.7%. The greater the delivery rates of the attack pattern, the accuracy results increased.

Keywords: LRDDoS, SD-IoT, Random Forest, Logistic-Regression, Machine Learning

1. Introduction

Currently, IoT technology is developing rapidly. IoT is widely used in various sectors, including Smart Home, Smart City, Smart Health, Smart Agriculture, Smart Manufacturing, and other sectors [1]. IoT devices do not have user interfaces, computing resources, and storage media that is functioned to implement firewalls and other diagnostic tools [2]. This makes IoT devices have security holes that can be exploited by attackers to weaken the communication process between IoT servers and users' devices [3]. The attack model that is commonly applied to weaken communication is to send a DDoS attack [4, 5].

One possible solution to overcome the problem of distributed system management in IoT networks is to integrate it with the SDN architecture. The combination of SDN with IoT is known as SD-IoT [6, 7]. The SDN control layer has a role as a traffic management center as well as an Intrusion Detection System (IDS) module to resolve security holes in IoT networks. The function of the SDN in general acts as a network traffic facilitator capable of managing resources as well as IoT network security [8, 9]. The SDN architecture allows the IoT network to separate the control and data delivery areas at different abstraction layers [10].

However, the centralized logic control on SDN is also still vulnerable to DDoS attacks [11]. DDoS is one of the attacks that is aimed to overwhelm the SDN centralized management system. This attack is performed by sending dummy packets continuously which can overwhelm the controller on the SDN and can even consume its computing resources [12, 42]. DDoS attacks have two types, namely high rate and low rate. High-Rate DDoS (HRDDoS) has the characteristics of the traffic that is sending data packets massively within a certain period, so it is relatively easier to detect while Low-Rate DDoS (LRDDoS) is very difficult to detect, because the attacks are hidden in normal data streams [14]. Therefore, LRDDoS is a major concern in SDN security issues which requires a system that can identify and detect these attacks comprehensively [15].

In previous research, several methods have been proposed to detect and mitigate HRDDoS and LRDDoS attacks. In research [16] a DDoS detection system has been built in SDN based on the Machine Learning methods by applying the Support Vector Machine

Accepted: 17-02-2022 | Received in revised: 03-04-2022 | Published: 20-04-2022

(SVM) algorithm (Linear and Radial Basis Function), K-Nearest Neighbor (KNN), Decision Tree (DTC), Random Forest (RF), Multi-Layer Perceptron (MLP), and Gaussian Naïve Bayes (GNB). Among these algorithms, SVM was the most efficient method with around 100% accuracy, precision, and recall. The authors were focused to detect the HRDDoS attack by deploying the DDoS attacks using high packet sending rates. The extracted features were originated from the OFPT_PACKET_IN message and port statistic provided by the OpenFlow standard.

Research [17] proposed an LRDDoS attack detection system using Machine Learning approaches. The features were extracted from the OpenFlow packages on two groups, namely, stateful features (with or without raw IP packet-based features) and stateless features. The authors also compared the results with traditional IP packet classification for DDoS attacks on IoT networks without SDN integration. At the testing phase, the researchers used 4 algorithms, including SVM, GNB, KNN, and RF. The researcher utilized the dataset from the OpenFlow on the SDN controller and switch which was made independently. The collected dataset has a total of 204,888 and 48,509 data containing normal traffic such as Internet Control Message Protocol (ICMP) messages, Hypertext Transfer Protocol (HTTP), Hypertext Transfer Protocol (HTTPS), Message Queuing Telemetry Transport (MQTT), the attack traffic containing a large number of Transmission Control Protocol Synchronization (TCP SYN) messages, and TCP retransmissions other than those contained in the normal stream. The experimental results for the GNB algorithm, accuracy, recall, and F1-score showed a percentage of 97% on the controller. The precision of the SVM and KNN algorithms was 96% and the precision of the RF algorithm was 97%. The NAM algorithm had the worst effect on switch, while the RF algorithm had the best effect. The accuracy, precision, recall, and F1-score of the RF algorithm were 91%, 95%, 94%, and 94%, respectively. The SVM and KNN algorithms had the best recall rate of 95%.

Research [18] used the SVM algorithm in DDoS detection as a learning model and combines it with the Kernel Principal Component Analysis feature selection technique (KPCA). The function of the KPCA implementation had a target to speed up the training time and to produce good accuracy. The results of the study showed that the feature selection technique using KPCA worked very effectively which could increase the accuracy by up to 98.97%. Furthermore, in research [19], researchers proposed a DDoS attack detection system based on Hybrid Machine Learning by combining two algorithms including SVM and Self Organized Map (SOM). The results of combining the two algorithms produced an attack detection accuracy of 96.77%.

In addition, several studies have also adopted Deep Learning techniques in the DDoS detection process. The method used in this study [20] applied a Deep Learning-based Low-Rate DDoS attack detection approach on an SDN network using the Hybrid Convolutional Neural Network-Long-Short Term Memory (CNN-LSTM) model. The results of the CNN-LSTM Hybrid model reached more than 99%.

Based on the previous research, the contributions made in this paper include proposing the use of Machine Learning with RF algorithms on the SD-IoT network for detecting the LRDDoS attacks deployed using the Constrained Application Protocol (CoAP) and a new dataset scheme using 21 features to be selected with Feature Importance - Logistic Regression. The Feature Importance method was aimed to reduce the computation load during the data preprocessing phase, to reduce the computational load during classification, and is also expected to increase the results of accuracy, precision, recall, and F1.

2. Research Methods

2.1 Emulation Topology

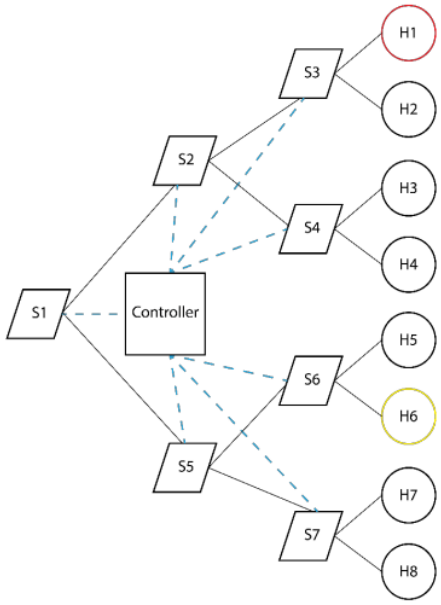


Figure 1. Emulation Topology

The experiment was emulated in a tree topology as shown in Figure 1, consisting of one RYU Controller [21], seven Open Virtual Switch (OvS) supporting the OpenFlow v.1.3.0 [22] (S1-S7), and eight hosts (H1-H8). The emulation process utilized the mininet-IoT emulator [23]. The research scheme was divided into three packet transmission speeds per second, namely 50, 100, and 200 packets per second (pps). During the

DOI: https://doi.org/10.29207/resti.v6i2.3878

experiment's scenario, H1 was named as an attacker who sent LRDDoS attack packets in the form of *.pcap files [24]. The number of attack packets is 39,994 data consisting of randomly generated Internet Protocol (IP) and Media Access Control (MAC) source address configurations sent using TCPReplay tools [25]. The dummy packets were received by H6 which was pointed as the victim (CoAP server [26]), activated its port on 5683.

2.2 Data Extraction Process and Data Preprocessing

Based on Figure 2, the flow of the extraction process originated from the proposed method was began by sending the LRDDoS attack packet via *.pcap file directed to the victim (H6). Furthermore, the incoming packets were filtered by the SDN switch based on the packet header's information and the SDN switch performed the actions or responses based on the appropriate rules defined by the SDN controller.

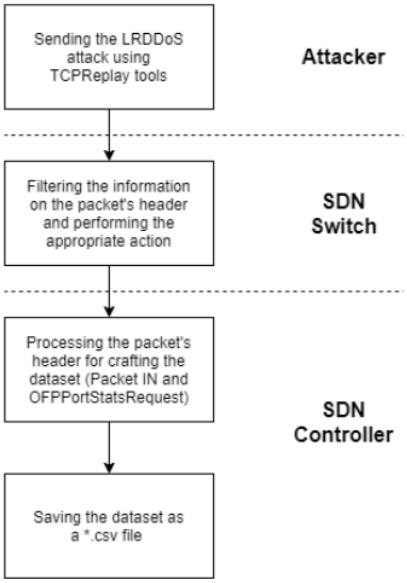


Figure 2. Block Diagram for Extracting the Dataset

Because the incoming packet consisted of randomly generated header information, it was considered as new data. The SDN switch automatically sent the packet to the controller encapsulated in the OFPT_PACKET_IN message (Table-miss event). Subsequently, the controller processed the packet header based on the appropriate information for the dataset (IPv4 header, TCP/UDP, and Port Statistics) and saved it in the form of a *.csv file as a dataset for the model generation and testing process.

The dataset used in this research was a new dataset scheme [27] that was created independently by the researcher by utilizing the features of the Openflow protocol. The dataset was retrieved through the information extraction process on the OFPT_PACKET_IN, Internet Protocol version 4 (IPv4), Transmission Control Protocol (TCP), User Datagram Protocol (UDP) headers, and several statistical information on switch's port where the incoming packet was captured. Statistical information was extracted via the OFPPortStatsRequest feature replies which could be sent from the controller to the SDN switches [28, 29]. The number of datasets used in this research was 160,006 packets as training data and 39,994 packets as test data, with a 50:50 ratio between LRDDoS attack packets and normal packets for avoiding an imbalanced dataset. There were 21 features available on the dataset. The list of features can be seen in Table 1.

Table 1. Feature's List

Feature's Name	Feature's Origin
datapath_id	OFPT_PACKET_IN
version	IPv4's Header
header_length	IPv4's Header
tos	IPv4's Header
total_length	IPv4's Header
flags	IPv4's Header
offset	IPv4's Header
ttl	IPv4's Header
proto	IPv4's Header
sum	IPv4's Header
src_ip	IPv4's Header
dst_ip	IPv4's Header
src_port	UDP's/TCP's Header
dst_port	UDP's/TCP's Header
port_no	OFPPortStatsReply
rx_bytes_ave	OFPPortStatsReply (rx_bytes / rx_packets)
rx_error_ave	OFPPortStatsReply (rx_bytes / rx_packets)
rx_dropped_ave	OFPPortStatsReply (rx_bytes / rx_packets)
tx_bytes_ave	OFPPortStatsReply (tx_bytes / tx_packets)
tx_error_ave	OFPPortStatsReply (tx_bytes / tx_packets)
tx_dropped_ave	OFPPortStatsReply (tx_bytes / tx_packets)

The Feature Importance method - Logistic Regression Coefficient functioned as a feature selector to obtain relevant features for the classification results [30, 31]. The features used in the classification process were only selected features that had a coefficient value not equal to 0 (less than 0 or more than 0). The coefficient value which had a non-zero value could increase the results of accuracy, precision, recall, and F1 score, while the coefficient value of 0 in the feature did not affect the classification results, the feature only burdened the SDN controller which then slowed down the feature selection process. The flow of the feature selection process can be seen in Figure 3.

DOI: https://doi.org/10.29207/resti.v6i2.3878

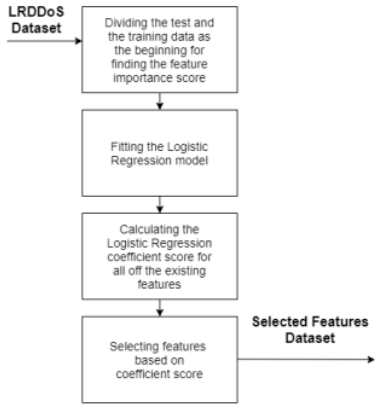


Figure 3. Block Diagram for Feature Selection's Process

2.3. LRDDoS Attack on SD-IoT

LRDDoS is categorized as an attack that is carried out in a distributed manner over normal network traffic, therefore LRDDoS is very difficult to detect. In this paper, the SDN architecture offered a solution to increase the security from LRDDoS attacks. In the SD-IoT framework, the SD-IoT controller was responsible for the centralized management system of all of the IoT devices.

The LRDDoS attack scheme is illustrated in Figure 4. The process was started with the attacker sending an attack package to the victim. The packet was going through the SDN switch for the process of matching the packet's header information with all of the flow rules that existed in the flow table. If there was one flow rule that had a flow match structure that corresponded to the packet header information, the switch automatically applied the action according to the flow action defined by the controller using the OFPT_FLOW_MOD message. Examples of actions that could be performed include forwarding packets through certain ports, blocking packets by not taking any action, forwarding packets to the controller if a table miss event occurs, and even direct response to the incoming packets.

However, if the packet did not match all of the flow match components, then the packet was encapsulated into an OFPT_PACKET_IN message and the message was sent to the controller. When the message was received by the controller, the controller performed the packet's inspection by opening the packet header information and matching it with the host information database that was directly connected to the topology where the controller was located.

As a form of response, the controller sent an OFPT_PACKET_OUT message containing new packets that have not been stored in the database with the aim of receiving the response from the destination host. When the destination host replied to the OFPT_PACKET_OUT broadcast/multicast packet from the controller, the controller indirectly had a delivery path mapping between the requesting host and the response message sender. If it already had a delivery path, the controller sent out an OFPT_FLOW_MOD message to instruct the data sending device (SDN switch) to install a flow rule as a medium for sending and determining the transmission path.

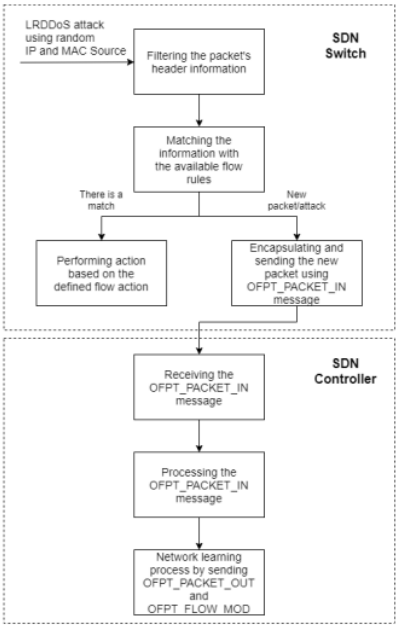


Figure 4. LRDDoS Attack's Block Diagram in SD-IoT

In the LRDDoS attack, the controller indirectly received a large number of new packets. The controller received many new packets because each packet had randomly generated MAC and IP source addresses. This circumstance forced the controller to process each of the OFPT_PACKET_IN packets burdening the controller's computational performance. If the computational load increased significantly, then scalability problems could re-emerge in the SD-IoT architecture.

2.4. Classification Process

The DDoS classification mechanism on the SDN network was begun by filtering data packets that entered the SDN switch. Furthermore, due to the construction of data packets consisting of random IP and MAC sources, the incoming data packets were categorized as new data and sent directly to the controller or can be referred to as Table-Miss Event. The sent packet was encapsulated in the OFPT_PACKET_IN message [32, 33]. In the controller, the incoming packet was parsed according to the header for each data.

DOI: https://doi.org/10.29207/resti.v6i2.3878

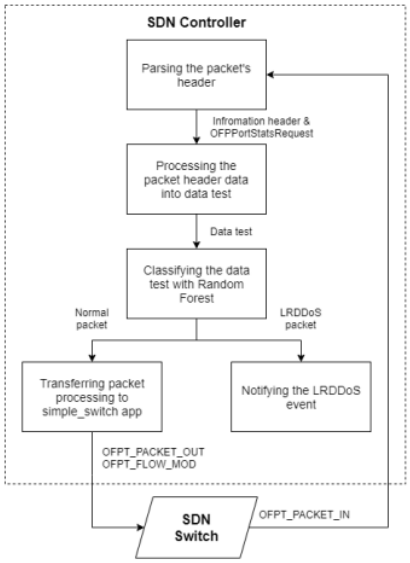


Figure 5. Flowchart of the Classification Process

Subsequently the header information was converted to a float data type using the StandardScaler function (Sklearn Python) to turn the package into a dataset. The next stage was the classification process using machine learning with the RF algorithm. However, before entering the classification process, the dataset was selected with feature importance - Logistic Regression Coefficient so that it could increase the accuracy of the classification results [34, 35].

When the incoming packet was detected as a normal packet, the data was forwarded back to the SDN switch and was handled by the simple switch application. However, if the application classifies the incoming packet as an LRDDoS attack, a notification appears informing the LRDDoS attack existed. Figure 5 is a flow chart of the explanation above.

3. Results and Discussions

Table 2. Logistic Regression Results

Feature's Name	Logistic Regression Coefficient Value
total_length	-1.6172
flags	6.7658
csum	-0.00195
src_ip	-1.85064
src_port	-0.26961
port_no	-0.08737
rx_bytes_ave	3.0446
tx_bytes_ave	0.08789

Based on the experiment according to the scenarios that had been made, the obtained results showed the values of the evaluation variables namely, accuracy, precision, recall, and F1 score that could be used to measure the effectiveness of the RF algorithm as a model in the detection and identification process of the LRDDoS attacks where the data test consisted of 39,994 dummy data in total. The data had 21 features only a few features were used for the emulation process.

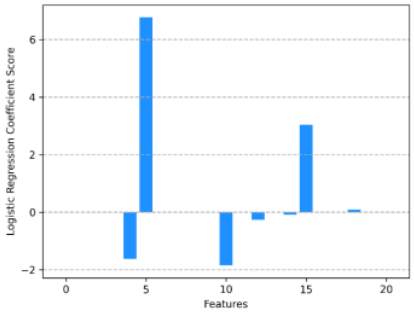


Figure 6. Graph of All Logistic Regression Results

The feature selection process was carried out by calculating the value of feature importance - Logistic Regression Coefficient. The results of the feature importance implementation obtained eight relevant features with the thorough details described in Table 2. These features had an influence on the training results, while the other 13 features did not affect the training results because they received only a 0 score of coefficient value. The magnitude of the feature coefficient could be interpreted as the relevance of these features during the classification process (increasing or decreasing the classification results) [36]. Figure 6 is a graph obtained in the selection process using the feature importance approach. From the graph, the features used are only features that have a value not equal to 0 (less than 0 or more than 0).

3.1. Training Results without SD-IoT

Table 3 is the result of an experiment using 8 features without using SD-IoT showing the time used for the training process requires 0.422 seconds with the results of the accuracy, precision, recall, and F1 score pointed at 100% which was considered as the highest value on the percentage. The generated model during the training process was utilized by the SDN controller on the SD-IoT environment to perform the classification process.

Table 3. Model Training Results

Accuracy	Precision	Recall	F1 Score	Training Time (s)
100%	100%	100%	100%	0.422

3.2. Classification Results in SD-IoT

In the experiment using SD-IoT, the packet delivery rate per second was divided into 3 speeds including 50, 100, and 200 pps as shown in Table 4. In the 50 pps experiment, the prediction loss value was pointed at 98.5%, and the accuracy, precision, recall, and F1 Score were similarly achieved at 92.3%. The prediction loss on the experiments with 100 pps was obtained at 98.8%,

DOI: https://doi.org/10.29207/resti.v6i2.3878

with 98.2% value pointed for the accuracy, precision, recall, and F1 score respectively. The last scenario using 200 pps obtained 99.1% for the prediction loss and 98.7% for each of the accuracy, precision, recall, and F1 score result. The greater the percentage of the prediction loss, the higher the value of accuracy, precision, recall, and F1 score was obtained.

The occurrence of prediction loss was caused by the controller device that continued to classify the similar packet more than once. This could happen because the controller received a low rate and a consistent number of dummy packets from the attacker. Automatically, when a new packet entered the controller, the detection application was still triggered to classify the previous data. Because there was a loop on the classification process for resolving the similar packet repeatedly, the data that has been successfully categorized only consisted of a small fraction of the data test which could increase the values of accuracy, precision, recall, and F1 score along with the growth of packet sending rate. This pattern could have occurred since the emulation was performed on the Mininet-IoT environment which could also produce unstable results [37].

Table 4. The Classification Results on SD-IoT

Packet Sending Rate (pps)	Accuracy %	Precision %	Recall %	F1 %	Prediction Loss %
50	92.3	92.3	92.3	92.3	98.5
100	98.2	98.2	98.2	98.2	98.8
200	98.7	98.7	98.7	98.7	99.1

4. Conclusion

In SD-IoT networks, Low-rate DDoS attacks are still one of the most significant problems in terms of centralized management. The proposed contribution to this paper was the utilization of a new dataset scheme used in the emulation process that differed from previous studies. The experiment also implemented the feature selection using the Logistic Regression Coefficient. The Random Forest method used for low-rate DDoS prediction had the highest accuracy at 98.7% and gained prediction loss value at 99.1% with a packet's 200 pps. In terms of the future possible project, the author will develop an attack mitigation process from these results, so that it can be seen the effectiveness of the identification module is an Intrusion Prevention System (IPS). The predictions loss may be reduced significantly by implementing the external data classification without involving the SDN controller since it can be accessed through the Secure REpresentational State Transfer (REST) Application Programming Interface (API) command.

Acknowledgment

The authors expressed their deepest gratitude for the support provided by the Informatics Laboratory and Informatics Department at the University of Muhammadiyah Malang.

Reference

[1] J. Bhayo, S. Hameed, and S. A. Shah, "An Efficient Counter-Based DDoS Attack Detection Framework Leveraging Software Defined IoT (SD-IoT)," *IEEE Access*, vol. 8, 2020. https://doi.org/10.1109/ACCESS.2020.3043082

[2] G. Liu, W. Quan, N. Cheng, H. Zhang, and S. Yu, "Efficient DDoS attacks mitigation for stateful forwarding in Internet of Things," J. Netw. Comput. Appl., vol. 130, no. January, pp. 1–13, 2019. https://doi.org/10.1016/j.jnca.2019.01.006

[3] F. S. Dantas Silva, E. Silva, E. P. Neto, M. Lemos, A. J. Venancio Neto, and F. Esposito, "A taxonomy of DDoS attack mitigation approaches featured by SDN technologies in IoT scenarios," Sensors (Switzerland), vol. 20, no. 11, pp. 1–28, 2020. https://doi.org/10.3390/s20113078

[4] D. Yin, L. Zhang, and K. Yang, "A DDoS Attack Detection and Mitigation with Software-Defined Internet of Things Framework," IEEE Access, vol. 6, no. Mcc, pp. 24694–24705, 2018. https://doi.org/10.1109/ACCESS.2018.2831284

[5] F. A. Fernandes Silveira, F. Lima-Filho, F. S. Dantas Silva, A. De Medeiros Brito Junior, and L. F. Silveira, "Smart Detection-IoT: A DDoS Sensor System for Internet of Things," Int. Conf. Syst. Signals, Image Process., vol. 2020-July, pp. 343–348, 2020. https://doi.org/10.1109/IWSSIP48289.2020.9145265

[6] J. Wang, Y. Liu, W. Su, and H. Feng, "A DDoS attack detection based on deep learning in software-defined Internet of things," IEEE Veh. Technol. Conf., vol. 2020-November, 2020. https://doi.org/10.1109/VTC2020-Fall49728.2020.9348652

[7] N. N. Tuan, P. H. Hung, N. D. Nghia, N. Van Tho, T. Van Phan, and N. H. Thanh, "A DDoS attack mitigation scheme in ISP networks using machine learning based on SDN," Electron., vol. 9, no. 3, pp. 1–19, 2020. https://doi.org/10.3390/electronics9030413

[8] K. K. Karmakar, V. Varadharajan, S. Nepal, and U. Tupakula, "SDN-Enabled Secure IoT Architecture," IEEE Internet Things J., vol. 8, no. 8, pp. 6549–6564, 2021. https://doi.org/10.1109/JIOT.2020.3043740

[9] Y. W. Chen, J. P. Sheu, Y. C. Kuo, and N. Van Cuong, "Design and implementation of IoT DDoS attacks detection system based on machine learning," 2020 Eur. Conf. Networks Commun. EuCNC 2020, pp. 122–127, 2020. https://doi.org/10.1109/EuCNC48522.2020.9200909

[10] M. Fajar Sidiq, Akbari Basuki, and D. Rosiyadi, "MiTE: Program Penyunting Topologi Jaringan untuk Pembelajaran SDN," J. RESTI (Rekayasa Sist. dan Teknol. Informasi), vol. 4, no. 5, pp. 970–977, 2020. https://doi.org/10.29207/resti.v4i5.2473

[11] V. Deepa, K. M. Sudar, and P. Deepalakshmi, "Design of Ensemble Learning Methods for DDoS Detection in SDN Environment," Proc. - Int. Conf. Vis. Towar. Emerg. Trends Commun. Networking, ViTECoN 2019, pp. 1–6, 2019. https://doi.org/10.1109/ViTECoN.2019.8899682

[12] S. Dong and M. Sarem, "DDoS Attack Detection Method Based on Improved KNN with the Degree of DDoS Attack in Software-Defined Networks," IEEE Access, vol. 8, pp. 5039–5048, 2020. https://doi.org/10.1109/ACCESS.2019.2963077

[13] J. Cui, J. Zhang, J. He, H. Zhong, and Y. Lu, "DDoS detection and defense mechanism for SDN controllers with K-Means," Proc. - 2020 IEEE/ACM 13th Int. Conf. Util. Cloud Comput. UCC 2020, pp. 394–401, 2020. https://doi.org/10.1109/UCC48980.2020.00062

[14] W. Zhijun, X. Qing, W. Jingjie, Y. Meng, and L. Liang, "Low-Rate DDoS Attack Detection Based on Factorization Machine

in Software Defined Network," IEEE Access, vol. 8, pp. 17404–17418, 2020. https://doi.org/10.1109/ACCESS.2020.2967478

[15] M. Baskar, J. Ramkumar, C. Karthikeyan, V. Anbarasu, A. Balaji, and T. S. Arulananth, "Low rate DDoS mitigation using real-time multi threshold traffic monitoring system," J. Ambient Intell. Humaniz. Comput., no. 0123456789, 2021. https://doi.org/10.1007/s12652-020-02744-y

[16] F. Sumadi and C. Aditya, "Machine learning in openflow network: Comparative analysis of ddos detection techniques," Int. Arab J. Inf. Technol., vol. 18, no. 2, pp. 221–226, 2020. https://doi.org/10.34028/IAJIT/18/2/11

[17] H. Cheng, J. Liu, T. Xu, B. Ren, J. Mao, and W. Zhang, "Machine learning based low-rate DDoS attack detection for SDN enabled IoT networks," Int. J. Sens. Networks, vol. 34, no. 1, pp. 56–69, 2020. https://doi.org/10.1504/ijsnet.2020.109720

[18] K. S. Sahoo et al., "An Evolutionary SVM Model for DDOS Attack Detection in Software Defined Networks," IEEE Access, vol. 8, pp. 132502-132513, 2020. https://doi.org/10.1109/ACCESS.2020.3009733

[19] V. Deepa, K. M. Sudar, and P. Deepalakshmi, "Detection of DDoS Attack on SDN Control plane using Hybrid Machine Learning Techniques," in 2018 International Conference on Smart Systems and Inventive Technology (ICSSIT), 2018, pp. 299-303. https://doi.org/10.1109/ICSSIT.2018.8748836

[20] B. Nugraha and R. N. Murthy, "Deep Learning-based Slow DDoS Attack Detection in SDN-based Networks," in 2020 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN), 2020, pp. 51-56. https://doi.org/10.1109/NFV-SDN50289.2020.9289894

[21] D. Y. Setiawan, S. N. Hertiana, and R. M. Negara, "6LoWPAN Performance Analysis of IoT Software-Defined-Network-Based Using Mininet-IoT," IoTaIS 2020 - Proc. 2020 IEEE Int. Conf. Internet Things Intell. Syst., pp. 60–65, 2021. https://doi.org/10.1109/IoTaIS50849.2021.9359714

[22] H. E. Wahanani, M. Idhom, and E. P. Mandyartha, "Equal cost multipath ryu controller analysis in software-defined networking," Proceeding - 6th Inf. Technol. Int. Semin. ITIS 2020, pp. 115–118, 2020. https://doi.org/10.1109/ITIS50118.2020.9321069

[23] X. Huang, Y. Tang, Z. Shao, Y. Yang, and H. Xu, "Joint Switch-Controller Association and Control Devolution for SDN Systems: An Integrated Online Perspective of Control and Learning," IEEE Trans. Netw. Serv. Manag., vol. 18, no. 1, pp. 315–330, 2021. https://doi.org/10.1109/TNSM.2020.3044674

[24] F. Hussain, S. G. Abbas, U. U. Fayyaz, G. A. Shah, A. Toqeer, and A. Ali, "Towards a Universal Features Set for IoT Botnet Attacks Detection," Proc. - 2020 23rd IEEE Int. Multi-Topic Conf. INMIC 2020, 2020. https://doi.org/10.1109/INMIC50486.2020.9318106

[25] G. Zheng, X. Xu, and J. Yan, "SD-CRF: A DoS Attack Detection Method for SDN," Int. Conf. Commun. Technol. Proceedings, ICCT, vol. 2020-October, pp. 1116–1120, 2020. https://doi.org/10.1109/ICCT50939.2020.9295801

[26] S. Arvind and V. A. Narayanan, "An Overview of Security in CoAP: Attack and Analysis," 2019 5th Int. Conf. Adv. Comput. Commun. Syst. ICACCS 2019, pp. 655–660, 2019. https://doi.org/10.1109/ICACCS.2019.8728533

[27] Sumadi, Fauzi (2022), "Low Rate DDoS (MQTT)", Mendeley Data, V1. https://doi.org/10.17632/bzf9jcvhx4.1

[28] Z. Li, W. Xing, S. Khamaiseh, and D. Xu, "Detecting Saturation Attacks Based on Self-Similarity of OpenFlow Traffic," IEEE Trans. Netw. Serv. Manag., vol. 17, no. 1, pp. 607–621, 2020. https://doi.org/10.1109/TNSM.2019.2959268

[29] N. Ahuja, G. Singal, D. Mukhopadhyay, and N. Kumar, "Automated DDOS attack detection in software defined networking," J. Netw. Comput. Appl., vol. 187, no. May, p. 103108, 2021. https://doi.org/10.1016/j.jnca.2021.103108

[30] A. S. Soma, T. Kubota, and H. Mizuno, "Optimization of causative factors using logistic regression and artificial neural network models for landslide susceptibility assessment in Ujung Loe Watershed, South Sulawesi Indonesia," J. Mt. Sci., vol. 16, no. 2, pp. 383–401, 2019. https://doi.org/10.1007/s11629-018-4884-7

[31] H. M. Rizeei, B. Pradhan, M. A. Saharkhiz, and S. Lee, "Groundwater aquifer potential modeling using an ensemble multi-adoptive boosting logistic regression technique," J. Hydrol., vol. 579, no. September, p. 124172, 2019. https://doi.org/10.1016/j.jhydrol.2019.124172

[32] A. M. D. Tello and M. Abolhasan, "SDN Controllers Scalability and Performance Study," 2019, 13th Int. Conf. Signal Process. Commun. Syst. ICSPCS 2019 - Proc., 2019. https://doi.org/10.1109/ICSPCS47537.2019.9008462

[33] W. Ma, J. Beltran, D. Pan, and N. Pissinou, "Placing Traffic-Changing and Partially-Ordered NFV Middleboxes via SDN," IEEE Trans. Netw. Serv. Manag., vol. 16, no. 4, pp. 1303–1317, 2019. https://doi.org/10.1109/TNSM.2019.2946347

[34] R. Santos, D. Souza, W. Santo, A. Ribeiro, and E. Moreno, "Machine learning algorithms to detect DDoS attacks in SDN," Concurr. Comput. Pract. Exp., vol. 32, no. 16, pp. 1–14, 2020. https://doi.org/10.1002/cpe.5402

[35] Naveen Bindra and Manu Sood, "Detecting DDoS Attacks Using Machine Learning Techniques and Contemporary Intrusion Detection Dataset," Autom. Control Comput. Sci., vol. 53, no. 5, pp. 419–428, 2019. https://doi.org/10.3103/S0146411619050043

[36] M. Saarela and S. Jauhiainen, "Comparison of feature importance measures as explanations for classification models," SN Appl. Sci., vol. 3, no. 2, pp. 1–12, 2021. https://doi.org/10.1007/s42452-021-04148-9

[37] H. M. Noman and M. N. Jasim, "POX Controller and Open Flow Performance Evaluation in Software Defined Networks (SDN) Using Mininet Emulator," *IOP Conference Series: Materials Science and Engineering*, vol. 881, no. 1, p. 012102, 2020/07/01 2020. https://doi.org/10.1088/1757-899x/881/1/012102

DOI: https://doi.org/10.29207/resti.v6i2.3878

LRDDoS Attack Detection on SD-IoT Using Random Forest with Logistic Regression Coefficient

ORIGINALITY REPORT

18%	13%	14%	5%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to Universitas Islam Indonesia Student Paper	2%
2	Submitted to Telkom University Student Paper	2%
3	joiv.org Internet Source	1%
4	academic-accelerator.com Internet Source	1%
5	A. Droos, Q. A. Al-Haija, M. Alnabhan. "Lightweight detection system for low-rate DDoS attack on software-defined-IoT", 6th Smart Cities Symposium (SCS 2022), 2022 Publication	1%
6	acta.uni-obuda.hu Internet Source	1%
7	Beny Nugraha, Rathan Narasimha Murthy. "Deep Learning-based Slow DDoS Attack Detection in SDN-based Networks", 2020 IEEE Conference on Network Function	1%

Virtualization and Software Defined Networks (NFV-SDN), 2020
Publication

8	android.googlesource.com Internet Source	1 %
9	Umar Islam, Abdullah Al-Atawi, Hathal Salamah Alwageed, Muhammad Ahsan, Fuad A. Awwad, Mohamed R. Abonazel. "Real-Time Detection schemes for Memory DoS(M-DoS) Attacks on Cloud Computing Applications", IEEE Access, 2023 Publication	1 %
10	Abdullah Ahmed Bahashwan, Mohammed Anbar, Iznan Husainy Hasbullah, Ziyad R. Alashhab, Ali Bin-Salem. "Flow-Based Approach to Detect Abnormal Behavior in Neighbor Discovery Protocol (NDP)", IEEE Access, 2021 Publication	<1 %
11	www.jurnal.iaii.or.id Internet Source	<1 %
12	par.nsf.gov Internet Source	<1 %
13	Novendra Setyawan, Nur Alif Mardiyah, Mas Nurul Achmadiah, Rusdhianto Effendi, A. Jazidie. "Active fault tolerant control for missing measurement problem in a Quarter	<1 %

car model with linear matrix inequality approach", 2017 International Electronics Symposium on Engineering Technology and Applications (IES-ETA), 2017
Publication

---

14 sc.judiciary.gov.ph
Internet Source
<1%

---

15 Samer Y Khamaiseh, Izzat Alsmadi, Abdullah Al-Alaj. "Deceiving Machine Learning-Based Saturation Attack Detection Systems in SDN", 2020 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN), 2020
Publication
<1%

---

16 Sukhveer Kaur, Krishan Kumar, Naveen Aggarwal, Gurdeep Singh. "A comprehensive survey of DDoS defense solutions in SDN: Taxonomy, research challenges, and future directions", Computers & Security, 2021
Publication
<1%

---

17 Worku Gachena Negera, Friedhelm Schwenker, Taye Girma Debelee, Henock Mulugeta Melaku, Yehualashet Megeresa Ayano. "Review of Botnet Attack Detection in SDN-Enabled IoT Using Machine Learning", Sensors, 2022
Publication
<1%

---

assets.researchsquare.com

18	Internet Source	<1%
19	ebin.pub Internet Source	<1%
20	Babita Majhi, Prastavana. "An Improved Intrusion Dectection System using BoT-IoT Dataset", 2022 IEEE 11th International Conference on Communication Systems and Network Technologies (CSNT), 2022 Publication	<1%
21	jyx.jyu.fi Internet Source	<1%
22	pempek.unsri.ac.id Internet Source	<1%
23	prr.hec.gov.pk Internet Source	<1%
24	researchportaltest.northumbria.ac.uk Internet Source	<1%
25	www.freepatentsonline.com Internet Source	<1%
26	"Inventive Communication and Computational Technologies", Springer Science and Business Media LLC, 2022 Publication	<1%

27	Da Yin, Lianming Zhang, Kun Yang. "A DDoS Attack Detection and Mitigation With Software-Defined Internet of Things Framework", IEEE Access, 2018 Publication	<1 %
28	Fauzi Dwi Setiawan Sumadi, Christian Sri Kusuma Aditya, Ahmad Akbar Maulana, Syaifuddin Syaifuddin, Vera Suryani. "Semi-supervised approach for detecting distributed denial of service in SD-honeypot network environment", IAES International Journal of Artificial Intelligence (IJ-AI), 2022 Publication	<1 %
29	Jayasree Sengupta, Sushmita Ruj, Sipra Das Bit. "A Comprehensive Survey on Attacks, Security Issues and Blockchain Solutions for IoT and IIoT", Journal of Network and Computer Applications, 2020 Publication	<1 %
30	Muhammad Waqas Nadeem, Hock Guan Goh, Yichiet Aun, Vasaki Ponnusamy. "A Recurrent Neural Network based Method for Low-Rate DDoS Attack Detection in SDN", 2022 3rd International Conference on Artificial Intelligence and Data Sciences (AiDAS), 2022 Publication	<1 %
31	Walid I. Khedr, Ameer E. Gouda, Ehab R. Mohamed. "FMDADM: A Multi-Layer DDoS	<1 %

	Attack Detection and Mitigation Framework Using Machine Learning for Stateful SDN-Based IoT Networks", IEEE Access, 2023 Publication	
32	Zhiyuan Li, Weijia Xing, Samer Khamaiseh, Dianxiang Xu. "Detecting Saturation Attacks Based on Self-Similarity of OpenFlow Traffic", IEEE Transactions on Network and Service Management, 2020 Publication	<1 %
33	dergipark.org.tr Internet Source	<1 %
34	insightsociety.org Internet Source	<1 %
35	repositor.umm.ac.id Internet Source	<1 %
36	repositorio.unb.br Internet Source	<1 %
37	researchrepository.ucd.ie Internet Source	<1 %
38	studyres.com Internet Source	<1 %
39	www.american-cse.org Internet Source	<1 %
40	www.hindawi.com Internet Source	<1 %

41	www.mdpi.com Internet Source	<1%
42	Abdullah Ahmed Bahashwan, Mohammed Anbar, Selvakumar Manickam, Taief Alaa Al-Amiedy et al. "A Systematic Literature Review on Machine Learning and Deep Learning Approaches for Detecting DDoS Attacks in Software-Defined Networking", Sensors, 2023 Publication	<1%
43	"Internet of Things and Analytics for Agriculture, Volume 3", Springer Science and Business Media LLC, 2022 Publication	<1%
44	"Security and Privacy in Digital Economy", Springer Science and Business Media LLC, 2020 Publication	<1%
45	Ahamed Aljuhani. "Machine Learning Approaches for Combating Distributed Denial of Service Attacks in Modern Networking Environments", IEEE Access, 2021 Publication	<1%
46	François De Keersmaeker, Yinan Cao, Gorby Kabasele Ndonda, Ramin Sadre. "A Survey of Public IoT Datasets for Network Security Research", IEEE Communications Surveys & Tutorials, 2023 Publication	<1%

Exclude quotes	On	Exclude matches	Off
Exclude bibliography	On		