DETECTION AND MITIGATION OF DISTRIBUTED DENIAL OF SERVICE ATTACKS ON NETWORK ARCHITECTURE SOFTWARE DEFINED NETWORKING USING THE NAIVE BAYES ALGORITHM

Misbachul Munir [1] **, Ipung Ardiansyah** [2] **, Joko Dwi Santoso** [3] **, Ali Mustopa** [4] **, Sri Mulyatun** [5]

[1),2),3), 4), 5)] *Department of Computer Engineering Universitas Amikom Yogyakarta*

email : misbachul.munir@students.amikom.ac.id [1)] , ipung.19@students.amikom.ac.id [2)] , jds@amikom.ac.id [3)] , ali.m@amikom.ac.id [4)] , sri.m@amikom.ac.id [5)]

Abstraksi

Serangan DDoS adalah bentuk serangan yang dilakukan dengan mengirimkan paket secara terus menerus ke mesin bahkan jaringan komputer. Serangan ini akan mengakibatkan mesin atau sumber daya jaringan tidak dapat diakses atau digunakan oleh pengguna. Serangan DDoS biasanya berasal dari beberapa mesin yang dioperasikan oleh pengguna atau bot, sedangkan serangan Dos dilakukan oleh satu orang atau satu sistem. Dalam penelitian ini, istilah yang akan digunakan adalah istilah DDoS untuk merepresentasikan serangan DoS atau DDoS. Dalam dunia jaringan, Software Defined Network (SDN) merupakan paradigma yang menjanjikan. SDN memisahkan bidang kontrol dari bidang penerusan untuk meningkatkan programabilitas jaringan dan manajemen jaringan. Sebagai bagian dari jaringan, SDN tidak luput dari serangan DDoS. Dalam penelitian ini, kami menggunakan algoritma naïve Bayes sebagai metode untuk mendeteksi serangan DDoS pada arsitektur jaringan Software Defined Network

***Kata Kunci* :**
Software-Defined Networking, Algoritma Naïve Bayes, DDoS, Kontrol Aliran

Abstract

DDoS attacks are a form of attack carried out by sending packets continuously to machines and even computer networks. This attack will result in a machine or network resources that cannot be accessed or used by users. DDoS attacks usually originate from several machines operated by users or by bots, whereas Dos attacks are carried out by one person or one system. In this study, the term to be used is the term DDoS to represent a DoS or DDoS attack. In the network world, Software Defined Network (SDN) is a promising paradigm. SDN separates the control plane from forwarding plane to improve network programmability and network management. As part of the network, SDN is not spared from DDoS attacks. In this study, we use the naïve Bayes algorithm as a method to detect DDoS attacks on the Software Defined Network network architecture

***Keywords* :**
Software-Defined Networking, Naïve Bayes Algorithm, DDoS, Flow Control

Introduction

Software-Defined Network (SDN) is a technology that changes the current network architecture paradigm that still combines the data plane and control plane into one in a router or switch device[1]. The characteristic of SDN is to separate data planes such as hardware such as switches or router and control plane which is often called controller[2][3][4]. So to configure a network architecture with multiple device scales to be dynamic and efficient[5][6]. SDN Architecture is divided into three layers, namely the application layer, the controller layer, and the infrastructure layer [4][7]. Inside the application layer is an application that is used to build traffic such as ids, load balancing and so on. The controller layer contains configurations based on rules that have been made which will be applied in the data plane. Whereas in the data plane consists of network devices such as routers and switches that are used to forward data packets [8].

SDN architecture is divided into three layers, namely the application layer, the control layer, and the infrastructure layer[4][7]. Inside the application, the layer is applications that are used to build traffic such as IDs, load balancing and so on. The controller layer contains a configuration based on rules that have been created that will be applied to data fields. Whereas in the field of data consists of network devices such as routers and switches that are used to forward data packets[8]. To connect between layers using an API consisting of two types, namely the API to the north to connect the control layer with the application layer and the API to the south is used to connect the control layer with the infrastructure layer[9].

Inside the controller layer and Soundbooth API, there is a core technology from SDN namely OpenFlow. OpenFLow is an SDN technology that

separates data fields from control fields. In the control field, there is an OpenFlow Switch which functions to manage the flow table provided by the OpenFlow Controller. While OpenFLow Controller is found in the Southbound API which functions to match content and commands regarding flow[1][3] [7].

SDN architecture has many benefits, one of which is security. The most common attack in network architecture is DDoS. DDoS attacks occupy the top of the threat list. DDoS attacks are attacks where various PC cloned frameworks attack resources, for example, servers, sites, or other system assets, and cause a denial of service for other clients who access resources[8]. In SDN, DDoS attacks can be classified into three categories namely infrastructure layer attacks, control layer attacks, and application attacks[7]. In this riset, we focus on the detection and mitigation of DDoS attacks using the Naive Bayes Algorithm

Related Works

After conducting a comprehensive study and analysis of several papers on the detection and mitigation of DDoS attacks on the SDN network, we examined several research papers with several different techniques for DDoS detection and mitigation. The topic of this paper[11] uses the SHDA (Slow HTTP Defense Application) controller as a barrier to DDoS attacks on the server. SHDA updates the flow of rules to block traffic from attackers so that the webserver can maintain its normal operation. In this paper[8] uses a third- party application, iftop, which is a command line system tool that generates a list of frequently updated network connections. If there are repetitive packets sent from the same address and at the same time interval, iftop will send the address to the firewall to be processed according to the firewall rules that are applied. In this paper[1] introduces a time-based method of preventing DDoS attacks by collecting attack data packets together in the near future the attack packets will be sent to the flow collector to be processed and become a database. In addition, in another paper[12] describes the EDIP (Early Detection and Isolation Policy) methodology in reducing DDoS attacks with the help of a small number of proxies and using the concept of load balancing as a proxy for balancing if overloaded. This paper

[13] aims to identify APT by analyzing network traffic and finding dangerous activities, in this framework it is integrated together with SDN controllers and six security products and uses Mininet emulation. This paper describes a methodology that is capable of detecting legitimate flash and traffic and discusses the existing methodology to prevent DDoS attacks at the network layer together with the current methodology to prevent DDoS at the application layer. This paper[2] describes the use of hybrid algorithms (Support Vector Machine (SVM) and Self Organized Map (SOM)). This method is very superior in detecting DDOS attacks from both SVM and SOM algorithms. This paper [5] uses sFlow software that is applied to the switch or router and then the packet received is filtered by sFlow based on time intervals. This paper discusses DDoS attacks and various techniques that can be prevented. This paper [10] introduces SDN as a new paradigm for solving problems. SDN proactive DDoS Defense Framework (ProDefense).

Table.1. Detection Methods and Mitigation of DDoS attacks

No	Title	Method
1	Time-based DDoS detection and mitigation for SDN controller	Software Defined Network (SDN)
2	Detection of DDoS Attack on SDN Control plane using Hybrid Machine Learning Techniques	Hybrid Machine Learning Techniques
3	Design and Implementation of an OpenFlow-Based TCP SYN Flood Mitigation	TCPSYN Flood Mitigation
4	Simulation and performance analysis of Security issue Using Floodlight controller in Software Defined Network	Floodlight Controller
5	Real-time detection and mitigation of distributed denial of service (DDoS) attacks in software defined networking (SDN)	Software sFlow
6	Packet in Message Based DDoS Attack Detection in SDN Network Using OpenFlow	OpenFlow controller
7	Studying the DDoS Attack Effect over SDN Controller Southbound Channel	Southbound Channel
8	DDOS detection and denial using third party application in SDN	Iftop (alat monitor sistem baris perintah yang menghasilkan daftar koneksi jaringan)
9	Software-Defined Networking (SDN): Layers and Architecture Terminology	Software-Defined Networking
10	DDoS Attack Detection and Mitigation Using SDN: Methods, Practices,	Software-Defined Networking

	and Solutions	
11	SDN-Assisted Slow HTTP DDoS Attack Defense Method	MetodeSoftware DefinedNetwork (SDN)sebagai pengontrol SHDA
12	Proactive DDoS attack detection and isolation	Load Balancing dan EDIP
13	A framework for security enhancement in SDN-based datacenters	APT
14	A novel framework to detect and block DDoS attack at the application layer	Application layer dan flash traffic

Research Methodology

This research begins by designing a software architecture network defined networking using Mininet software as supporting software. The next stage is to configure the Mininet Software. The next step is testing the Software Defined Networking network architecture by carrying out a Distributed Denial of Service (DDoS) attack. The next stage is to classify the attack data class using the Naïve Bayes Classifier Algorithm and an analysis of the classification results to obtain knowledge. The steps taken in this study are in Figure 1.

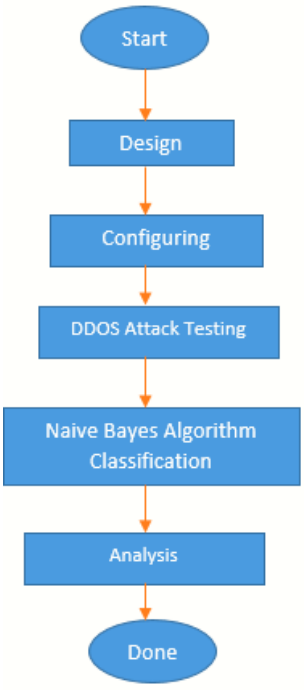

Figure. 1. Research Methodology

In design, researchers use the Mininet software. Which is a CLI based emulator that is used to create a Software Defined Network (SDN) network topology mininet is an open-source software that was intentionally made to facilitate the research and explanation of the SDN system. Minimizing the network using software that is actually a Linux kernel- based network can be used in SDN network testing.

At the configuration stage, researchers configure each topology in SDN FlowControl. The next step after completing configuration is the testing phase of DDoS attacks. Where trying to attack the SDN network architecture with very many packet requests at fast intervals. Shown in Figure 2 and Table 2 and Figure 3.

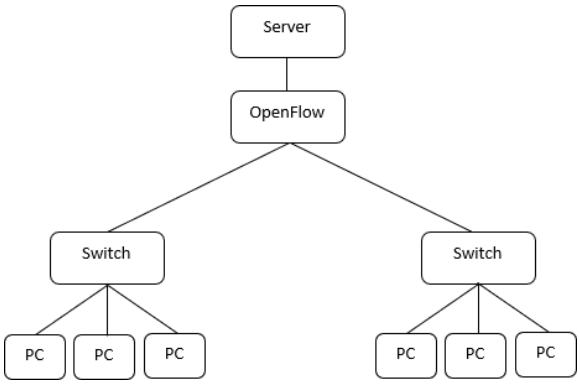

Figure. 2. SDC FlowControl Topology Architecture

Table.2. Specification Of SDN FlowControl

Platform	Ubuntu 16.04
Network emulator	Mininet 2.2.1
Controller	OpenFlow
Internet protocol	IPv4
Number of nodes	6
Number of server nodes	1
Number of attacker nodes	4

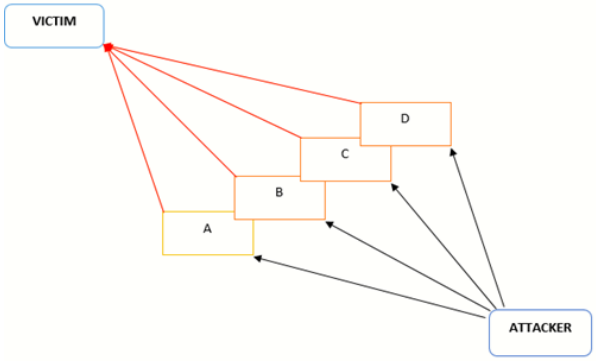

Figure. 3. DDoS Attack

The next step is to classify data classes from DDoS attacks using the Naïve Bayes Algorithm. Which is a method for predicting future probabilities based on past experience. The advantage of applying the Naïve Bayes classification algorithm is that it can reduce data noise in large datasets. Naive Bayes is used to classify the results for each given data set (test data) based on the dataset provided with accurate results (training decision data). Bayes' theorem is expressed mathematically as an equation.

$$P(A|B) = \frac{P(B|A)\ x\ P(A)}{P(B)}$$

Information:

Indicates A and B.

P (A) and P (B) are the possibilities of A and B P (A | B) is the probability that A is true

P (B | A) is the probability of B that A is true

After classifying the data class with naïve Bayes, then analyzing the results of the class classification.

Results And Discussion

Capturing packet captures packets that flow on the Software-Defined Network (SDN) network and the required details are stored. The package retrieval process can be modified by selecting options such as header-only complete package options. After the packet is captured, the number of packets is displayed and immediately predicted whether the packet was attacking or not. Statistical analysis shows the number of packets received from a particular type and also displays the cumulative network protocol ratio and the transport protocol ratio. The packet information received is used to analyze whether they are attacker packages or normal packages. The Naïve Bayes algorithm takes the training data set used to evaluate the package received. It only requires a little training data to do this, but they must be able to describe different scenarios. Shown in Figure 4 and Figure 5.

	Standard				Naïve Bayes			
sigma	1.5	2	2.5	3	1.5	2	2.5	3
FPR (%)	0.97	0.77	0.65	0.53	0.90	0.74	0.58	0.50
DR (%)	89.44	88.11	87.51	86.98	89.64	88.54	90.67	92.79
Accuracy (%)	89.67	88.38	87.29	87.28	92.34	91.67	92.05	89.17

Figure. 4. Comparison of the Comparative Detection Rate and False Positive Value between using naïve bayes and not using naïve bayes (Standard)

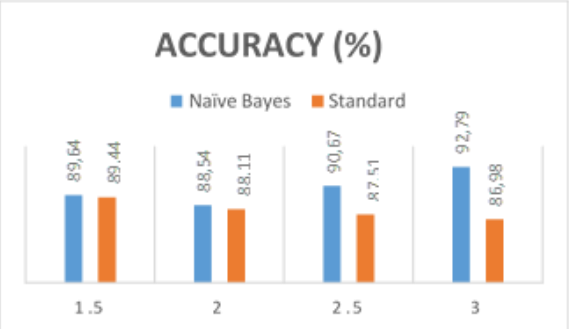

Figure. 5. The accuracy of detection of DDoS attacks uses naive and standard bayes

The proposed system can increase the detection rate and reduce the occurrence of false-positive alarms in the system to detect DDoS attacks using the Naïve Bayes classification. The system can detect DDoS attacks that occur on Software Define Network (SDN). In existing systems, false-positive rates decrease with increasing threshold and detection rates increase with an increasing threshold. The proposed system is capable of producing a small increase in DDoS detection rates compared to systems without naïve bayes. Thus increasing accuracy in detecting DDoS attacks on Software-Defined Networking networks.

Conclusions

In this study, the use of SDN networks is only in a simple topology with one type of DDoS attack. Prevention of DDoS in SDN using the naïve Bayes algorithm looks more accurate than DDoS prevention relying on the OpenFlow standard. But the naïve Bayes algorithm requires training data for the accuracy of packets received as attack packets or normal packets. For further research, it can use a more complex topology with many types of DDoS attacks and the application of the naïve Bayes algorithm uses more training data so that the detection accuracy is higher.

References

[1] N. I. G. Dharma, M. F. Muthohar, J. D. A. Prayuda, K. Priagung, and D. Choi, "Time-based DDoS detection and mitigation for SDN controller," 17th Asia-Pacific Netw. Oper. Manag. Symp. Manag. a Very Connect. World, APNOMS 2015, pp. 550–553, 2015.

[2] V. Deepa, K. M. Sudar, and P. Deepalakshmi, "Detection of DDoS Attack on SDN Control plane using Hybrid Machine Learning Techniques," 2018 Int. Conf. Smart Syst. Inven. Technol., no. Icssit, pp. 299–303, 2019.

[3] R. Nagai, W. Kurihara, S. Higuchi, and T. Hirotsu, "Design and Implementation of an OpenFlow-Based TCP SYN Flood Mitigation," Proc. - 6th IEEE Int. Conf. Mob. Cloud Comput. Serv. Eng. MobileCloud 2018, vol. 2018-Janua, pp. 37–42, 2018.

[4] R. Vedhapriyavadhana, E. Francy Irudaya Rani, and M. Theepa, "Simulation and performance analysis of Security issue Using Floodlight controller in Software Defined Network," 2018 Int. Conf. Emerg. Trends Innov. Eng. Technol. Res. ICETIETR 2018, pp. 1–6, 2018.

[5] B. H. Lawal and A. T. Nuray, "Real-time detection and mitigation of distributed denial of service (DDoS) attacks in software defined networking (SDN)," 26th IEEE Signal Process. Commun. Appl. Conf. SIU 2018, pp. 1–4, 2018.

[6] X. You, Y. Feng, and K. Sakurai, "Packet in Message Based DDoS Attack Detection in SDN Network Using OpenFlow," Proc. - 2017 5th Int. Symp. Comput. Networking, CANDAR 2017, vol. 2018- Janua, pp. 522–528, 2018.

[7] B. Mladenov, "Studying the DDoS Attack Effect over SDN Controller Southbound Channel," 10th Natl. Conf. with Int. Particip. Electron. 2019 - Proc., pp. 1–4, 2019.

[8] R. M. Thomas and D. James, "DDOS detection and denial using third party application in SDN," 2017 Int. Conf. Energy, Commun. Data Anal. Soft Comput. ICECDS 2017, pp. 3892–3897, 2018.

[9] E. Haleplidis, J. H. Salim, and D. Meyer, "'Software-Defined Networking (SDN): Layers and Architecture Terminology', RFC 7426, DOI 10.17487/RFC7426," no. June 2016, pp. 1–35, 2015.

[10] N. Z. Bawany, J. A. Shamsi, and K. Salah, "DDoS Attack Detection and Mitigation Using SDN: Methods, Practices, and Solutions," Arab. J. Sci. Eng., vol. 42, no. 2, pp. 425–441, 2017.

[11] K. Hong, Y. Kim, H. Choi, and J. Park, "SDN-Assisted Slow HTTP DDoS Attack Defense Method," IEEE Commun. Lett., vol. 22, no. 4, pp. 688–691, 2018.

[12] V. Kansal and M. Dave, "Proactive DDoS attack detection and isolation," 2017 Int. Conf. Comput. Commun. Electron. COMPTELIX 2017, pp. 334–338, 2017.

[13] M. Ammar, M. Rizk, A. Abdel-Hamid, and A. K. Aboul-Seoud, "A framework for security enhancement in SDN-based datacenters," 2016 8th IFIP Int. Conf. New Technol. Mobil. Secur. NTMS 2016, pp. 3–6, 2016.

[14] S. Sivabalan and P. J. Radcliffe, "A novel framework to detect and block DDoS attack at the application layer," IEEE 2013 Tencon - Spring, TENCONSpring 2013 - Conf. Proc., pp. 578–582, 2013.