DDoS Attacks Detection Based on ASVM in Software-Defined Networking

Abdussalam Alashhab

abdussalaam91@gmail.com

Omran ali ben Taher

omranbentaher@gmail.com

Faculty of Information Technology, Al-Asmarya University

Yousef Abudlla

abouadlla@gmail.com

Faculty of Information Technology, Al-Zawi University

Muhammad Yunis Daha

dahayounis@gmail.com

Department of Computer Science, University Technology Petronas

الملخص

أشارت الاهتمامات البحثية إلى أن الشبكات المعرفة بالبرمجيات (SDN) تتمتع بميزات عديدة مقارنة بالشبكات التقليدية. حيث ان مفهوم الشبكات المعرفة البرمجيات يقوم على فصل بيانات التحكم عن بيانات التوجيه ماديا في أجهزة الشبكة. لقد ثبت أن مفهوم الشبكات المعرفة بالبرمجيات كان قادرًا على حل بعض مشكلات الأمان، وخوارزمية آلة متجه الدعم (SVM) هي الخوارزمية الحالية التي ساعدت كثيرًا في حل بعض مشكلات الشبكة. ومع ذلك، فإن مفهوم الشبكات القائم على البرمجيات لا يزال عرضة لنقاط الضعف. من بين أهم التهديدات الأمنية التي تواجه استقرار الشبكة هو هجوم منع الخدمة الموزع (DDoS). في هذا العمل يتم اقتراح نموذج أمني قائم على خوارزمية آلة متجه الدعم المتقدمة (ASVM) لتكون بمثابة تحسين لخوارزمية (SVM) نظرًا لقدرتها العالية بالتعامل مع تعدد الفئات واكتشاف تهديدات هجوم (DDoS) من طبقة التحكم ومحولات (OpenFlow).

Abstract

Research interests have indicated over the years that software-defined network (SDN) has a great advantage over the traditional network. The benefit of SDN is the ability of the network control to be physically separated from forwarding devices. It has been established that SDN has been able to solve certain security issues, The support vector machine (SVM) algorithm is the existing algorithm that has helped a great deal to solve certain network issues. However, SDN is still prone to vulnerabilities. One of which is the distributed denial of service (DDoS) attacks. The advanced support vector machine (ASVM) is proposed in this research to serve as an enhancement to the SVM because of its ability to multiclass and detect DDoS attack threats from the control layer and OpenFlow switches in SDN.

Keywords: SDN, DDoS attack, Network Security, Machine Learning, SVM, ASVM.

1.0 INTRODUCTION

In recent times, technologies associated with networking, are developed for infrastructure that is advanced. With these recent developments, cloud services, server virtualization, and mobile services are the strongest point in a traditional network architecture. This often comes as a hierarchical arrangement in a client-server model. This trending technology which has surpassed the traditional applications can access different databases and servers in different network domains, it is therefore expected that it would be the case of multiple (clients and servers). It is also important to note that the traffic pattern may not be the same [1], however, businesses that entail both private and public cloud services are expected to provide agility to access applications and other It resources on demand. This then gave rise to software-defined networking (SDN) [2]. SDN provides a new concept of network infrastructure and with this, [3] it helps to solve the limitation of traditional networking. Furthermore, SDN has great advantages compared to the traditional means, it is not without its challenges and needed to be solved. [4] One of the biggest issues of SDN is a security issue, such as denial of service (DoS) attacks, distributed denial of service (DDoS) attacks.

The inflow of DDoS attacks has brought about various discrepancies in existing network services. This has in turn led to the economic meltdown and with bad consequences. The DDoS attack is one of the major security challenges affecting the network [4]. It is there pertinent to detect DDoS attacks in an accurate and quick way.

SDN is a trending architecture that differentiates the control plane from the data plane. SDN has unique characteristics such as; centralized control, is a programmable network and the interface is open. The attack on the network of DDoS is quite a high tech one, such as:

- It causes a lack of cooperation between the network nodes.
- Address fraud is usually used which makes it a challenge to trace it to the source of the attack.
- The response time is limited compared to the attack time.

Therefore, this has necessitated the need for advanced technologies such as ASVM to detect DDoS attacks on the control plane and data plane, in order to prevent an unnecessary attack on the SDN. The SVM initially is an existing algorithm in machine learning that is used by the existing system of SDN. However, there is a need to put an advancement to this algorithm to detect network attacks of DDoS attacks from the controller and OpenFlow switches.

This paper aims to propose, ASVM, as an advanced enhancement of an existing SVM algorithm to repel the DDoS attack from the control and data planes, [5] an attack such as DDoS can be detected by an algorithm that has a multivalued attribute, ASVM is proposed in this research to detect this threat in the SDN.

2.0 RELATED WORK

There are various techniques with which network attacks are detected in past according to researchers. There is a single technique that uses network behaviors and there is anomaly-based detection, and this uses machine learning techniques. However, there are according to [6] Artificial Neural Network (ANN) is used to detect both known and unknown DDoS attacks. Other machine learning techniques used for network attack detection are Fuzzy Logic (FL), Decision Tree (DT), Evolutionary algorithm, Navies Bayes (NB). Furthermore, according to [5] FL can be used for reach traffic detection of DDoS attacks on the SDN. Researchers have provided different solutions to the challenges of the OpenFlow protocol. Furthermore, research has been carried out on how to detect threats using the DT technique, and the location of the person responsible for the attack was detected [7, 8]. With this system, it is possible to detect attacks with a false alarm. Moreover, according to [9] SVM is used to classify the attacks which have normal traffic due to their high accuracy and less positive rate. SVM along with other techniques were compared for the detection of attack and SVM provided a more accurate classification than other techniques.

However, the SVM did not provide an accurate attack detection for the SDN [10]. It is important to note that the ASVM come in very useful as it is a technology is a new technology that can be used to solve various challenges and threat in SDN.

3.0 SDN AND DDoS DETECTION BASED ASVM

In this section, we justify the notion of SDN illustration, DDoS attacks detection based on ASVM, and explain ASVM work for classifying the threat that may be exploited SDN.

3.1 Software Defined Networks

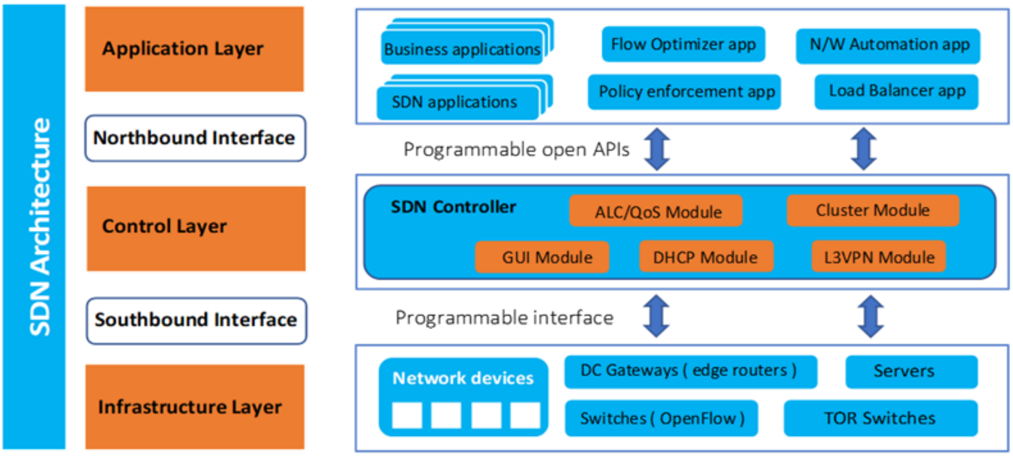

Figure 1. SDN Architecture [11].

Software-Defined Networking (SDN) simplifies network management by separating the control logic (the control plane) from the underlying hardware that redirects traffic (the data plane). This separation between the control plane and the data plane turns network adapters into simple forwarding devices, while the control logic and functions are implemented in a logically central controller. Figure 1 shows the basic architecture of SDN. Many open-source SDN controllers are available, including POX, NOX, Floodlight, and OpenDaylight. It's important to remember that a logical central SDN controller does not always imply a physical central system. Many SDN frameworks, such as ONOS and OpenDaylight, allow distributed frameworks. SDN's success has been demonstrated by the fact that it has been embraced for wide-area network management by organizations such as Google. SDN is a great option for the next generation of Internet architecture because of its unique qualities. The earliest and most extensively used SDN protocol is OpenFlow. The OpenFlow protocol specifies a method for the SDN controller to communicate directly with the data plane [11]. The controller sends packet processing rules to the OpenFlow switches' flow tables. The rule looks for traffic that satisfies its criteria and takes action, such as dropping, diverting, or changing it. The OpenFlow switch may act as a router, switch, firewall, load balancer, and more depending on the rules set up by the controller application. SDN is considered to be a perfect platform for the development of effective DDoS attack detection and mitigation systems. The separation of control and data layers, as well as the concept of flow-based traffic, considerably aid in the identification of attacks. Furthermore, having a single point of control allows for quick discovery. SDN's unique qualities have been used by researchers to boost security against classic attacks, such as DDoS attacks. Although the SDN architecture has the ability to construct powerful DDoS defenses, it also comes with the danger of vulnerabilities and failures due to controller attacks. Code injection attacks, man-in-the-middle attacks, and controller denial-of-service attacks are only a few examples. The effectiveness of SDN-based networks can be compromised by these attacks. However, in this paper, we focus on illustrating the features to improve security with SDN. We give a full review of the SDN-based ASVM method for detecting and mitigating DDoS attacks in this context. Based on our detection method, we also assess DDoS attack detection and mitigation solutions.

3.2 Advanced Support Vector Machine

The ASVM algorithm takes traffic data as input and determines whether or not a DDoS attack is created as a consequence. A multi-class support vector is used by ASVM. In the feature normalization step of the SVM algorithm, linear kernels, polynomials, radial kernel function kernels (Gaussian kernels), and sigmoidal kernels are commonly utilized. The Gaussian kernel function is employed in this suggested technique. Using a support vector in the input feature space, the Gaussian kernel may compute the exponential decay function. In the support-vector, it reaches its maximum value. The binary characteristics are ordered using the AVL tree structure when they are supplied. The AVL tree is a self-balancing binary search tree with re-balancing and length balancing capabilities. In the traditional SVM algorithm, Testing and training timeframes are dependent on the dataset's type and might take a lengthy period. Because of the height balancing characteristic of the AVL tree structure in ASVM, the testing time may be minimized. As a result, the suggested technique can increase the performance of the SVM classifier [12].

4.0 RESEARCH METHODOLOGY

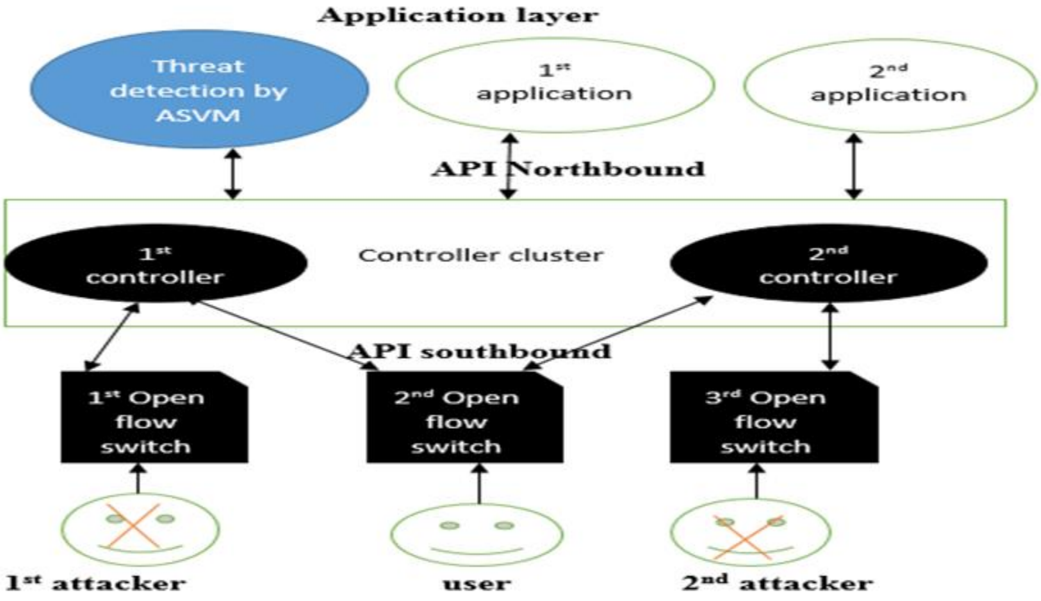

Figure 2. Proposed ASVM threat detection on SVM framework.

For this research, the ASVM is proposed as a methodology to detect DDoS attacks on the SDN. A framework to diagrammatically represent how message alert is derived immediately an attack is discovered [13] the proposed framework is engineered by various application concepts which have security requirements that differ. ASVM depends on the active nature of software-defined networking and also a robust protective mechanism. Every intending user or attacker in the SDN is expected to go through the OpenFlow switches, once this is done the details would be confirmed on the header fields which comprises of user/source IP address, source port, destination port, IP address for the destination, this details would cross-check to know if there are flow entries, once it is detected action is executed, in the case that there is none, the details will be forwarded to the controller via an application programming interface which s in Southbound using the information in a control message. It is important to note that controllers are connected as clusters and once traffics arrives, it is then forwarded to an application programming interface that is Northbound to detect threats ASVM application layer. Figure 2, indicates the framework for ASVM threat detection on SDN.

4.1 Traffic Detection

In order to detect an attack on SDN, the most important part is the traffic data collection. The details of traffic data can be obtained through an OpenFlow control which is from the OpenFlow switches [14, 15]. Usually, traffic data are saved in the flow table which happens to be within the OpenFlow switches. In order to extract the traffic data, the message is been responded to by the OpenFlow switch and in turn, sends the request message to the controller. Figure 3 indicates the steps by steps process of normal traffic generation [8]. A representation is given of how traffic information is being extracted from the switch in figure 4.

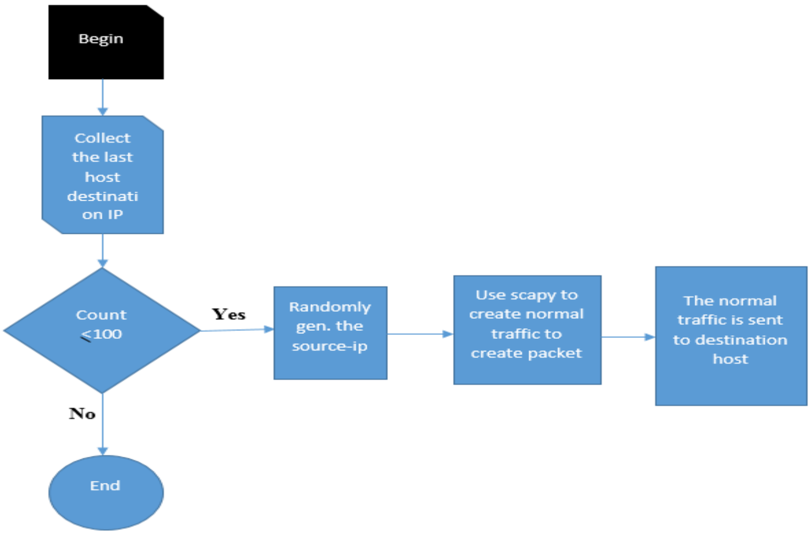
Begin
Collect the last host destination IP
Count <100
Yes
Randomly gen. the source-ip
Use scapy to create normal traffic to create packet
The normal traffic is sent to destination host
No
End

Figure 3 steps to generate normal traffic.

```
Mininet> sh ovs-ofctl dump-flows s1 nxst_flow reply (xid=0x4): cookie=0x0,
duration=165.700s, table=0, packets=8, n_bytes=560, idle_age=20, in_port=1
actions=flood
```

Figure 4 example of traffic flow details from a switch.

4.2 ASVM to Detect the DDoS attack on SDN Network Based

The proposed ASVM either classifies a packet as normal traffic or an attack. SVM is a machine learning algorithm that is able to classify and regress attacks. [16, 17]. It is generally used in various areas due to its high accuracy, its strength in dealing with high-dimensional data, and its ability to model diverse data. SVM is initially used for linear

classification issues. It is assumed that there are two classes in a linear two classification issues which are +1 and -1, (class).
V denotes vector with components, Vi data set on n is indicated as;
D= {(Vi, Yi)} n when i=1, where Vi denotes the i the characteristic vector in a dataset and Yi, is the label associated with Vi. The value of Yi is +1 or −1.
There is a parallel line distinguishing the vector class of -1 from +1, which is denoted by;
w = v + b = 0.

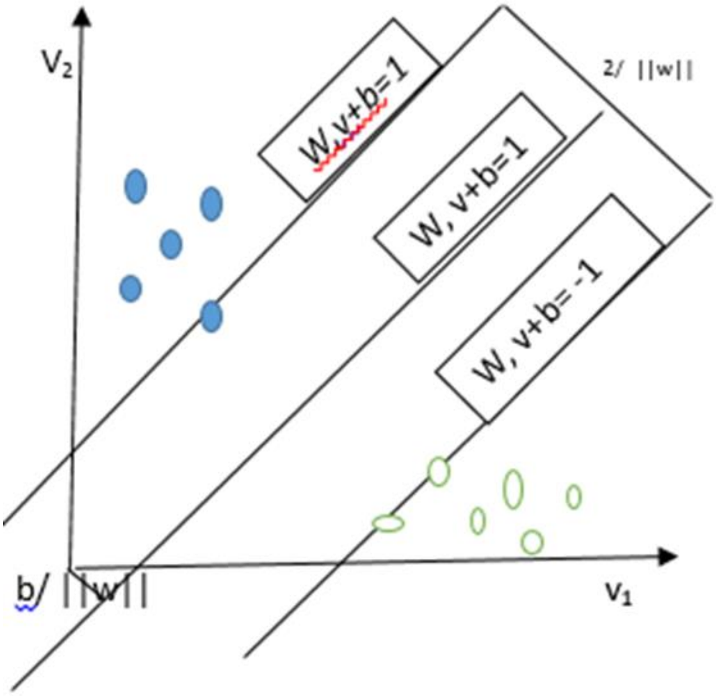

Figure 5 support vector machine (SVM).

W is regarded as weight vector and **b** which is scalar is referred to as bias. Class label 1 is regarded as **w = v+b** and that of class label -1 which happens to be beneath the straight line is regarded as **w = v = b-1**. In a situation where the dataset is linear separate, the two hyperplanes are seen as parallel and a reasonable distance must be given between them [18]. It is calculated as; **2/||w||.** Figure 5. indicates the above illustrations.
1≤ i ≤ n. this indicates that the problem of optimization is minimal. It is good to know that the maximization of margin may cause an error due to the misclassification of the data. In order to consider advanced vector machines, the slack variable should be put into consideration (e_i) and its classification error (A). The slack variable is the variable that measures the distance of the point to its marginal hyperplanes [19]. The equation below indicate the problem.
Minimize $\|w\|^2/2 + A \sum e_i$ where i=1.

Subject to $y_i(w, v_i - b) \geq 1$ e_i , e_i ≥ 0.

Classification error, c>0, indicates the benefits of margin maximization and minimizing the amount of slack. It is necessary to consider the classier judgment one-to-one and one-to-some in multiclass classification [8, 9].

5.0 Conclusion

In this proposed research, an advanced support vector system was proposed as a way to detect DDoS attacks in SDN on the OpenFlow switches by the SDN controller, DDoS attacks are detected based on the ASVM algorithm. The introduction of ASVM has also solved challenges such as; lack of cooperation between two coherent nodes, it has prevented the use of fraud addresses in the controller plane, ASVM is a multiclass algorithm and also is able to detect the attack on SDN almost immediately. This has therefore outgrown traditional ways of detecting DDoS attacks as it is a more effective way of detecting attacks in SDN.

References

[1] F. Tang, P. Tinno, P. A. Guti´errez, and H. Chen, “e benefits ˇ of modelling slack variables in SVMs,” Neural Computation, vol. 27, no. 4, 2015.

[2] S. H. Mujtiba and G. R. Beigh, “Impact of DDoS attack (UDP flooding) on queuing models,” in Proceedings of the 2013 4th

[3] International Conference on Computer and Communication Technology (ICCCT), Allahabad, India, September 2013.

[4] Conference: Innovations on Communication $eory, INCT, Istanbul, Turkey, October 2012.

[5] S. Acharya and N. Tiwari, “Survey of DDoS attacks based on TCP/IP protocol vulnerabilities,” IOSR Journal of Computer Engineering, vol. 18, no. 3, pp. 68–76, 2016.

[6] H. Harshita, “Detection and prevention of ICMP flood DDOS attack,” International Journal of New Technology and Research (IJNTR), vol. 3, no. 3, pp. 63–69, 2017.

[7] S. Rajneet, “A study of DoS & DDoS-smurf attack and preventive measures,” International Journal of Computer Science and Information Technology Research, vol. 2, no. 4, 2014.

[8] T. Lukaseder, G. Shreya, and K. Frank, “Mitigation of flooding and slow DDoS attacks in a software-defined network,” in Proceedings of Cryptography and Security, Santa Barbara, CA,USA, August 2018.

[9] A. Verma and D. Kumar Xaxa, “A survey on HTTP flooding attack detection and mitigating methodologies,” International Journal of Innovations and Advancement in Computer Science, vol. 5, no. 5, 2016.

[10] F. Yihunie, A. Eman, and A. Odeh, “Analysis of ping of death DoS and DDoS attacks,” in Proceedings of IEEE Long Island Systems, Applications and Technology Conference (LISAT), Farmingdale, NY, USA, May 2018.

[11] Ubale, T., & Jain, A. K. (2020). Survey on DDoS attack techniques and solutions in software-defined network. In *Handbook of computer networks and cyber security* (pp. 389-419). Springer, Cham.

[12] Oo, M. M., Kamolphiwong, S., & Kamolphiwong, T. (2017, November). The design of SDN based detection for distributed denial of service (DDoS) attack. In *2017 21st International Computer Science and Engineering Conference (ICSEC)* (pp. 1-5). IEEE.

[13] A. Akamai, Memcached Reflection Attacks: A NEW era for DDoS, Akamai Technologies, Cambridge, MA, USA, 2018.

[14] F. Keti and S. Askar, “Emulation of software defined networks using mininet in different simulation environments,” in Proceedings of the 6th

International Conference on Intelligent Systems, Modeling, and Simulation, Kuala Lumpur, February 2015.

[15] A. Moore, "Cross-validation for detecting and preventing overfitting," 2001.

[16] M. Bogdanoski, A. Risteski, and T. Shuminoski, "TCP SYN flooding attack in wireless networks," in Proceedings of the

[17] L. Tauber, "Introducing the normal distribution in a data analysis course: specific meaning contributed by the use of computers," in Proceedings of the ICOTS 6 : the Sixth International Conference on Teaching Statistics, Cape Town, South Africa, 2002.

[18] S. Asadollahi, B. Goswami, and A. M. Gonsai, "Implementation of SDN using OpenDayLight controller," in Proceedings of the International Conference on Recent Trends in IT Innovations-Tecafe ´ , vol. 52, no .2, India, April 2017.

[19] B. Pfaff, "Open vSwitch," 2014, http://www.openvswitch.org//support/slides/brkt.pdf.