IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

# INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

## IN COMPUTER & COMMUNICATION ENGINEERING

Volume 10, Issue 5, May 2022

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.165

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 5, May 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1005319 |

# Protection against DDos Attack Using SOM Algorithm

**Ms.Pooja.P.Dhere, Prof. Gayatri Bhandari**

Department of Computer Engineering, JSPM'S Bhivarabai Sawant Institute of Technology and Research, Pune, India

Department of Computer Engineering, JSPM'S Bhivarabai Sawant Institute of Technology and Research, Pune, India

**ABSTRACT:** Software-defined network (SDN) is a network architecture that used to build, design the hardware components virtually. We can dynamically change the settings of network connections. In the traditional network, it's not possible to change dynamically, because it's a fixed connection. SDN is a good approach but still is vulnerable to DDoS attacks. The DDoS attack is menacing to the internet. To prevent the DDoS attack, the machine learning algorithm can be used. The DDoS attack is the multiple collaborated systems that are used to target the particular server at the same time. In SDN control layer is in the center that link with the application and infrastructure layer, where the devices in the infrastructure layer controlled by the software. In this paper, we propose a machine learning technique namely Decision Tree and Support Vector Machine (SVM) to detect malicious traffic. Our test outcome shows that the Decision Tree and Support Vector Machine (SVM) algorithm provides better accuracy and detection rate.

## I. INTRODUCTION

DDos, commonly abbreviated as Distributed Denial of Service, is used to wash out the network resources. The end-user cannot get access to the essential information and also makes the application's performance very slow. DDos attempts to make a webapplication or online service busy by congestion with massive floods of traffic produced from several multiple resources. It is hard to locate where the attack comes from or the origin of the attack because it arrives from various sources, usually uses Trojon to infect a system.SDN architecture improves the network performance by decoupling the network control and forward function. The control programs running in a logically centralized controller will control multiple routers across the network. If an anomaly is detected, the controller is instructed by the application to reprogram the data plane to alleviate it. Both control and data plane runs on routers that are distributed across the network, where the devices have open interfaces that can be controlled by the software. The application layer is used to configure network devices. The control layer (control plane) which consists of the same controller it is the brain of the SDN architecture. These two layers are communicated through API.

### *A. MOTIVATION*

- **Financial motivations:** The most prevalent motivation behind an attack is financial gain. Cybercriminals are able to ransom or extort businesses with unprotected web systems and applications who want to avoid being attacked or wish to stop an attack. Often requesting hard to acquire bitcoins as payment with the ransom being increased by the day if a business can't pay. This can lead to hours, if not days of downtime of e-commerce and other business critical applications
- **Non-financial motivations:** Of the many non-financial reasons a cybercriminal might launch an attack the most common include a protest or "hacktivism" against a business practice or organizations whose ideologies differ from theirs. For example, groups such as Anonymous have been known to attack businesses who have been affiliated with political candidates, have been deemed to be controlling the internet and even medical organizations for what they feel is questionable medical care of minors.
- **Cover for targeted attacks:** Another motivation that we are seeing more frequently is that a DDoS attack is used as cover for other more sophisticated targeted attacks. According to a Computer Weekly article published in October 2016, "The majority of DDoS attacks (53%) resulted in additional compromise, including viruses (46%), ransomeware (15%) and other malware (37%)." This same report found that 21% of these attacks resulted in customer data theft.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 5, May 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1005319 |

*B. Objectives*

1. As most of the DOS attack detection system are triggered by high rate traffic.
2. According to the characteristics of periodicity and short burst in DOS at a lowrate ,it is hard to detect into the network.
3. Comparing the different Detection techniques for the DOS attack at a low rate, and finding the appropriate detection technique to mitigate the attack having low false rate.

## II. REVIEW OF LITERATURE

[1]Smart grid networks require reliable local detection schemes to detect intrusions. In the literature.
[2]Huang H B, Hong L, Chang-Yue Y U, et al. Analysis on Ukraine Power Grid Blackout and Its Enlightenment of ICSinChina[J].StandardScience,2016
[3] Eunsuk Kang et al. used a Markov chain-based game analysis model to propose a real-time detection scheme for false data injection attacks in smart grids. This scheme lacks coverage
of common attack types of the grid. In the literature
[4], an improved CUSUM intrusion attack detection method based on Bloom Filter address statistics for dynamic threshold update is proposed.
[5] The method collects grid traffic data in the data collection phase, and then performs intrusion behavior judgment. The attack detection method based on alarm data fusion has proposed by Yanan Sun.conforms to the heterogeneous characteristics of the grid, thus eliminating the deviation of the simple physical layer detection method or the simple information layer detection method. But this method can only determine that the line is abnormal and cannot locate the specific attacked node. And this method requires additional host devices to deploy Snort, and the security of the host device will also affect the detection results.
[6] In this paper the vulnerability of the route maintenance phase of the wireless Mesh network DSR (Dynamic Source Routing) protocol is used, and the corresponding attack method is designed for the network protocol. Wang K et al.
[7] proposed using the Bayesian honeypot game model to solve the shortcomings of the traditional honeypot technology detection dynamic attack ability

## III. PROPOSED METHODOLOGY

### A. SMART GRID DOS INTRUSION DETECTION METHOD

1. According to the design pattern of smart grid and the characteristics of DoS attack, this paper designs a smart grid intrusion detection structure based on machine learning.
2. Aiming at the existing design structure of smart grid, this paper uses the attack vulnerabilities of smart meters and data servers to add data acquisition and intrusion detection modules between smart meters and data servers.
3. Real-time data acquisition and detection in the smart grid is realized. When DoS attack behavior is detected, the alarm system is activated to perform alarm processing.
4. The typical attack methods of DoS are smurf, neptune, teardrop, pod, land and so on. DoS attacks make the resources of smart grid unavailable. It achieves the goal of attack by blocking communication or consuming network bandwidth.
5.By repeatedly sending a large number of useless requests to smart meters or collectors.

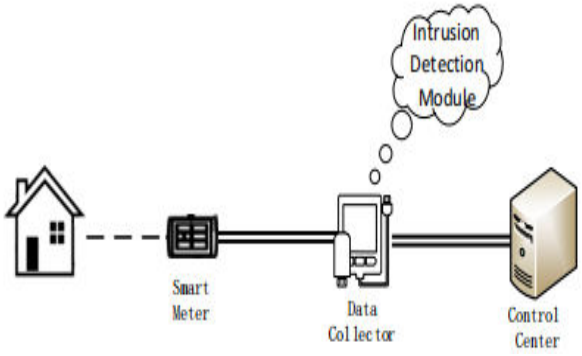


Fig.1Smart grid intrusion detection architecture diagram

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 5, May 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1005319 |

**B. SVM and Decision tree algorithm**

. In this section, we discuss about our proposed work for identifying DDoS attacks using ML in SDN. We have usedSVM and Decision tree algorithm to detect the attacks dueto its accurate classification and less complexity.

. The DDoS attack mainly categorized into three types such as :

(i) volume-based attack, which is mainly used to use drench the internet pipe of targeted server like UDP floods and ICMP floods

(ii) protocol attacks like SYN flood, fragmented packet, ping of death, smurf DDoS which mainly focus on extracting the server resources

(iii) application layer attacks include GET/POST floods which focus on web applications and its goal is to crash the web.

## III. MACHINE LEARNING

A) SDN consists of three planes such as data plane, control plane and application plane. Data plane carries the network traffic based on the decision made by controller. Control plane decides the flow of traffic by computing the routing tables.
B) Application plane manages the other applications like load balancer, firewalls, Quality of Service (QoS) applications etc.
C) SDN architecture improves the network performance by decoupling the network control and forward function. The control programs running in a logically centralized controller will control multiple routers across the network.
D) The SDN provides the sole ability to the applications to get to know the entire network information. During high traffic, the integration of different applications helps for load balancing and intrusion detection.
E) If an anomaly is detected, the controller is instructed by the application to reprogram the data plane to alleviate it. Both control and data plane runs on routers that are distributed across the network, where the devices have open interfaces that can be controlled by the software.
F) In SDN architecture, it is possible to reconfigure the multiple devices at the same time. The application layer is used to configure network devices. The control layer (control plane) which consists of the same controller it is the brain of the SDN architecture.
G) These two layers are communicated through API. The infrastructure layer (data plane) that communicates between the controller and the network devices use a central protocol. Figure 2 explains about the SDN architecture. Since huge amount of traffic is passing through the controller, proper security mechanism is essential to analyze and identify suspicious traffic.
H) We propose machine learning-based mechanism to identify the malicious activities in the SDN binvestigating the traffic features.

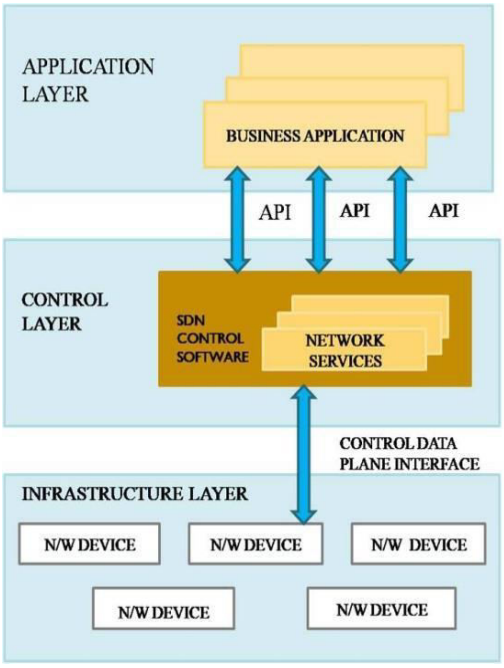


Fig 2. SDN Architecture

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 5, May 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1005319 |

*A. Mathematical Model*

The System Implementation plan table, shows the overall schedule of tasks compilation and time duration required for each task.

## IV. EXPERIMENT SETUP

- A self-organizing map (SOM) or self-organizing feature map (SOFM) is an unsupervised machine learning technique used to produce a low-dimensional (typically two-dimensional) representation of a higher dimensional data set while preserving the topological structure of the data.
- For example, a data set with *p* variables measured in *n* observations could be represented as clusters of observations with similar values for the variables. These clusters then could be visualized as a two-dimensional "map" such that observations in proximal clusters have more similar values than observations in distal clusters.
- This can make high-dimensional data easier to visualize and analyze.

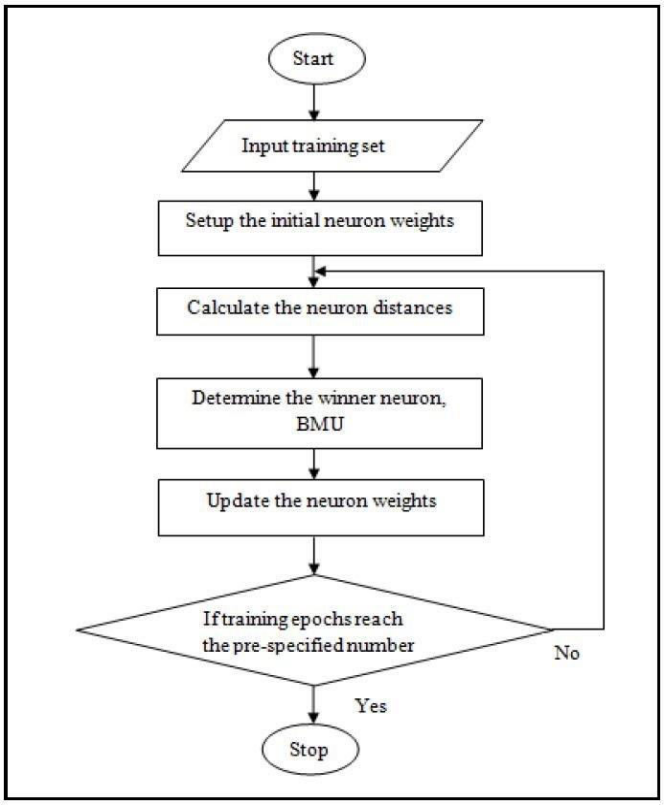


Fig 3. SOM Algorithm Flowchart

## V. CONCLUSION

SOM represents Self-Organizing Feature Map. It is a clustering and data visualization technique depends on a neural network viewpoint. Regardless of the neural network basis of SOM, it is simply presented-minimum in the context of the alteration of prototype-based clustering.

**The algorithm of SOM is as follows −**

1. Initialize the centroids.
2. repeat

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 5, May 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1005319 |

3. Choose the next object.
4. Determine the closest centroid to the object.
5. Refresh this centroid and the centroids that are close, i.e., in a definite neighborhood.
6. until the centroids don't change much or a threshold is outspace.
7. Create each object to its nearest centroid and restore the centroids and clusters.

A) **Initialization** − This step (line 1) can be implemented in multiple ways. One method is to select each element of a centroid randomly from the range of values observed in the data for that element.

While this method works, it is not essentially the best method, especially for making rapid convergence. Another method is to randomly select the original centroids from the accessible data points. This is very much like randomly choosing centroids for K-means.

B) **Selection of an object** − The first step in the loop (line 3) is the choice of the next object. This is simple, but there are several difficulties. Because convergence can require some steps, each data object can be used several times, particularly if the multiple objects is small. But if the number of objects is large, then not each object required to be used. It is also applicable to improve the influence of specific groups of objects by improving their frequency in the training set.

C) **Assignment** − The determination of the nearest centroid (line 4) is easy, although it needed the description of a distance metric. The Euclidean distance metric is utilized, as is the dot product metric. When utilizing the dot product distance, the data vectors are generally normalized beforehand and the reference vectors are normalized at every step. In this method, using the dot product metric is same to using the cosine measure.

D) **Update** − The update step (line 5) is difficult. Let m1..., mk, be the centroids. For time step t, let p(t) be the current object (point) and consider that the nearest centroid to p(t) is mj. Therefore, for time t+1, the jth centroid is refreshed by using the following equation.

*E)* **Termination** − It is determining when it is adequate to a stable set of centroids is an essential issue. Ideally, iteration must continue until convergence appears, that is, until the reference vectors do not change or change small. The cost of convergence will based on a multiple factors, including the data.

## REFERENCS

[1]Vidyaev I G, Ivashutenko A S, Samburskaya M A. Smart Grid Concept As A Modern Technology For The Power I ndustry Development.
[2]Huang H B, Hong L, ChangYue Y U, et al. Analysis on Ukraine Power GridBlackout and Its Enlightenment of ICS in China[J]. Standard Science, 2016.
[3]Jianye Hao, Eunsuk Kang, Jun Sun, Zan Wang, “An Adaptive Markov Strategy for Defending Smart Grid False Dat a Injection from Malicious Attackers”,IEEE Transactions on Smart Grid. Sept. 2016.
[4]Jiaxuan Fei,Tao Zhang,Yuanyuan Ma,Cheng Zhou. A DDoS attack detectionmethod for power grid industrial contr ol system based on BF-DT-CUSUM algorithm[J]. Telecommunications Science.2015 (12).
[5]Yanan Sun, Xiaohon Guan, Ting Liu, Yang Liu, “A cyberphysical monitoring system for attack detection in smart grid ”, Computer Communications Work-shops 2014.
[6] Wang K, Du M, Maharjan S, et al. Strategic Honeypot Game Model for Distributed Denial of Service Attacks in the Smart Grid[J]. IEEE
[7] Transactions on Smart Grid, 2017, PP(99):1-1.
[8] Pooja B, Pai M M M, Pai R M, et al. Mitigation of insider and outsider DoS attack against signature based .
[9] Saxena H, Richariya V. Intrusion Detection in KDD99 Dataset using
[10] SVM-PSO and Feature Reduction with Information Gain[J].
[11] International Journal of Computer Applications, 2014, 98(6):25-29 Sousa, P. H. F.; Nascimento, N. M. M.; Almeida, J. S.; Rebouças.
[12]Filho, P. P. and Albuquerque, V. H. C. (2019). Intelligent Incipient Fault Detection in Wind Turbines based on Industrial IoT Environment. Journal of Artificial Intelligence and Systems, 1, 1–19.authentication inVANETs[C]// Computer Aided System Engineering. IEEE, 2014:152-157.

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor: 8.165

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

# INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

## IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details