Wireless Personal Communications (2021) 116:2743–2757
https://doi.org/10.1007/s11277-020-08042-2

Improved Network Monitoring Using Software-Defined Networking for DDoS Detection and Mitigation Evaluation

J. Ramprasath[1] · V. Seethalakshmi[2]

Accepted: 23 December 2020 / Published online: 1 January 2021

Abstract

The Software-Defined Networking (SDN) is termed to be a promising paradigm since it provides a perfect administration for the network separating the data plane from the control plane. This is unlike the traditional network that has worked with the coupled data and the control plane that allows no scope for innovation. The decoupling of the forwarding and the control plane allows many advantages, such as a programmable control plane, migration, protocols, etc. Despite the provisions in the SDN that provides flexibility and agility in the performance of the network. The network environment suffers from security threats that occur due to DDoS. As the traditional methods prove to be insufficient for DDoS detection and mitigation since they lag in simple and autonomous management. The article presents the fast and flexible method for the early identification of the abnormal traffic flow for detecting the DDoS attacks and the mitigation techniques in SDN will reduce the severity of the DDoS attacks. The proposed method is simulated using the Mininet to show the proficiency of the system in terms of reliability, flexibility, processing overhead, cost, and throughput.

Keywords Software defined networking · Distributed denial of service · Abnormal traffic flow · DDoS detection · Mitigation

1 Introduction

The SDN is the most significant paradigm in handling the networks that are large and complex [1] by simplifying network management [7]. The traditional networks that worked along with the coupled data and the forwarding plane found difficulties in deploying the improved variants of the prevailing protocols. SDN offered the trail of the programmable network and seperates the forwarding and the control plane. This makes

✉ J. Ramprasath
jrprasath@gmail.com

V. Seethalakshmi
vseetha14@gmail.com

[1] Department of Information Technology, Dr.Mahalingam College of Engineering and Technology, Pollachi, India

[2] Department of Electronics and Communication Engineering, KPR Institute of Engineering and Technology, Coimbatore, India

the up-gradation of the prevailing protocols which is possible along with the flexible control [2]. The segregation between the data and the control plane by the SDN, makes the switches in the data plane to be simple forwarding devices. Providing a separate centralized control for the whole network for improving the network efficiency, and management [5], for enabling the easy andand flexible software development. The application of inventory network protocols and functions are possible [8] using SDN. Further, the separation of the control andand forward plane requires tiny information about the network to set up a perfect configuration and management by the controller [9]. The performance of the SDN along with the wireless-sensor makes them flexible, adaptable, and easily manageable for solving the innate problems of the wireless sensor networks [6, 24–26]. It effectively improvises the utilization of the network, decreasing the cost of the operation, and causing progressive growth and innovation. The SDN requires special traffic methods to be employed in the proper handling of the data and control traffic flow [10].

Dealing with SDN is termed to be a promising structure that enhances the network efficiency andand performance by completely controlling the operations of the network using a separate program. The SDN's for the cloud paradigm provides the agile andand flexible service providing progress in terms of intelligent worldwide connections, granular security, cost, and downtime reductions. Despite SDN capabilities provides efficient traffic flow management, managing of security threats, the attack detection using the entropy, the pattern analysis of the traffic, and the connection rate detection [19]. DoS attacks make the system unavailable for the users from transmitting an enormous amount of abnormal traffic directly to the server or the network towards the destination by a single node. The DDoS is a type of attack that is against the network, server, resources, and website by multiple computers sending the service request for the clients. Many traditional methods [16] employed in attack, detecting andand to perform the mitigation in the SDN environment has resulted with the insufficiency on dynamic DDoS attack detection andwhich causeshigher maintenance cost for the connection, state tables, packet marking, moreover, the additional devices are required for detecting the attacks [15]. So there arises a necessity for the fast and flexible method of early identification for the abnormal traffic flow and the method to reduce the severity of the DDoS attack in the SDN environment.

The article proposes a method to identify the abnormal traffic flow to detect the DDoS attacks and perform the mitigation on SDN environment for reducing the severity of the DDoS attacks and it also enables the users with the secure utilization of the resources. The large scale network with the possibility of showing a continuous performance uplift, by the SDN. It is liable for being attacked by the enormous abnormal traffic flow, causing the deterioration, the functioning networks are blocked and its service towards the clients crashing the intended system. The attack proceeded with the help of multiple computer systems towards the particular destination system is called the DDoS attack. The DDoS affects the performance of the network, hindering its services and thereby reducing the throughput, reliableness of the services, increasing the latency in the network services, and sometimes even denying the service of the request [27, 28]. The proposed works have significance in network monitoring that continuously keeps track of the traffic on the network and the detection of the abnormal traffic flow in the SDN environment. The framework of SDN reduces the severity to devise the network functioning along with the agility, flexibility, reduced processing overhead, and cost. This is done by employing three stages, Stage 1: Employing a double-fold tracking that keeps track of the normal and the abnormal traffic flow. Stage 2: Alleviation of the DDoS reducing the acuteness of the attack. Stage 3: Validation of the method to make sure the proposed system enables in having reliable service provisioning, that is flexible and agile.

The layout of the article is organized as follows. The related works in Sect. 2, which describes the details of the SDN and the DDoS affects the SDN along with the survey on the detection and the mitigation techniques. Section 3 presents the proposed method of early detection and mitigation. Section 4 gives the result evaluation. Section 5 provides the conclusion and future work for other malicious attacks.

2 Related Works

Hu et al. [1] the significance of the SDN along with the concepts, applications, language, quality of service, security, its incorporation with the wired and wireless networks. Nunes et al. [2] the programmable networks which including the SDN and its historical background to detect the attacks early, the architecture of the SDN along the prevailing and the proceeding future applications. Drutskoy et al. [3] the flexible network topology management of the SDN that sets a standard interface for the controlling and forwarding thus providing a platform of the virtualization aiding multitude of applications with the different topologies. Van et al. [4] the OpenNet monitoring using the SDN and the OpenFlow protocol communication between SDN controller and OpenFlow Switch. Kim et al. [5] the complex network management by maintaining the proper communication network that is challenging in the traditional scheme is easily done by using the SDN. It is implemented using the fine-tuned traffic metrics to enumerate whether the end-to-end QOS parameters are met. Luo et al. [6] the inabilities of the wireless sensor network adapt to the changing policies, and difficulties in network managing are addressed. The SD-WSN and the sensor OpenFlow are used to address the technical difficulties in the WSN. Farhady et al. [7] the technologies related to the SDN are reviewed, covering the three significant parts of the SDN, the application, control, and the data plane, with the future directions for the meaningful research. Li et al. [8] survey presents an up to date information about the existing OpenFlow-based SDN along with the security challenges and its remedy.

Pakzad et al. [9] the topology discovery challenges for the SDN is computed in the paper for applying simple modifications to the SDNwhich reduces overhead incurred and achieve better efficiency. Akyildiz et al. [10], the improvement in the capability of the SDN to have an overall view of the network, its status, with a perfect traffic control is presented in the paper to have better traffic control and managing, the research challenges of the traffic engineering are also addressed in the paper, Xiong et al. [11] the paper proposes the queuing replica of the OpenFlow on the grounds of the forwarding the packet and the traversing time of the average packets along with the analysis of the same using various parameters. Rai et al. [12] the types of the DDoS attacks are surveyed along with the spoof named as the attacking packets in the named data network switches. Rai et al. [13] the survey on the interest flooding attack affecting the pending interest table is to reduce the performance of the network along with the detection and the mitigation techniques are presented. Rao et al. [14] the paper address the defense measures for the DDoS of the internet service providers, the merits and the demerits of the defense measures along the enhancements of the future research. D’Cruze et al. [15] the SDN for the mitigating of the DDoS and surveyed the major traditional approaches, their limitations, flexibility and the efficiency of the effective automated solution for mitigating of the DDoS for the ISP. Carl et al. [16], identifying the DDoS successes, with an envision of the ability to detect the attacks and the techniques are surveyed in the article, the solution that the combination of the techniques would result with the optimal results for the identification were presented. Yan et al. [17], surveyed the SDN and malicious attacks leads to business loss and its remedies. Ahmed et al. [18] suggested the anomaly detection categorized into four types namely, classical, statistical, information theory, and clustering. Bawanyn et al. [19], the SDN used in the detection and the mitigation of the malicious DDoS and DoS attacks. Yan et al. [20] recommended that the enormous data growth lead to DDoS which is handled using the multilevel DDoS identification approaches on SDN.

D'Cruze et al. [15] surveyed that the DDoS initially starts with the attacker identifying the single system in the network that is unprotected against the attack and it leads to discovering the more unprotected systems in the same network. The attacker takes complete control of the unprotected systems in the network and floods the malicious traffic towards the destined network or the server or the domain and it leads to shutting down its services i.e. denying services to the clients. Yan et al. [17] These denying of service is categorized into three services based on the attack, as (i) DDoS attacks by flooding of packets, that overburden the resource in the target node the bandwidth available. (ii) DDoS attacks for the network or the transport layer due to the inadequacies in the protocol. (iii) DDoS attacks of the application layer overburdening the layer with the monstrous volume of the application request. All the above three categories cause a flooding of the packets to the target node or network, causing deterioration in the performance of the network by the denying of the task. The DDoS attacks any application in any network, which leads to business continuous loss.

3 DDoS Attack Detection and Mitigation in SDN Environment

The SDN enabled on a network, separates forwarding and the control plane that was previously coupled in the traditional networks into two layers, to have complete monitoring of the network actions. Therefore, the data (forwarding) layer is controlled by the set of protocols (programs) in the control layer, in the process of transmitting the data from the source to the destination. Moreover, the control plane holds the content table maintaining the details of the devices in the data layer along with the protocols and forwarding directory. The proposed method for the attack detection mechanism and the alleviation for reducing the severity of the attack takes a few strides such as the accumulation of the data for the perpetual tracking of the system, to identify the equipment with uncertain functioning and the abnormal data flow in the system. The abnormal traffic detection stage detects the abnormality on the packets flow, then with the alleviation techniques and later with the information centre that keeps the reports obtained for future use. Figure 1 illustrates the overall modules in the proposed system.

3.1 Data Accumulation

This is the first stage of the proposed systems to track the abnormalities in the traffic. The flow of the traffic is sent to the control layer from the data layer each time based on the request. The SDN controller periodically sends for the details of the flow of the traffic and accumulates the information of the traffic flow, once the traffic flow is received. The proposed

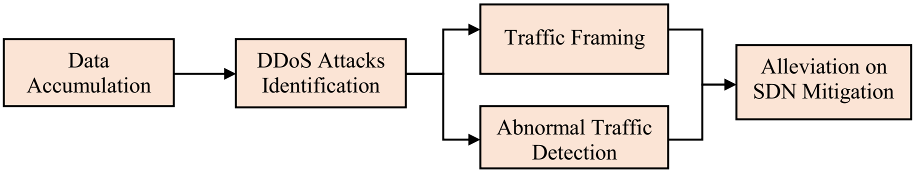

Data Accumulation
DDoS Attacks Identification
Traffic Framing
Abnormal Traffic Detection
Alleviation on SDN Mitigation

Fig. 1 Flow diagram for the proposed system

method selects the behavior of the traffic in terms of the total amount of the packets received in the (P_r) traffic, the total amount of the bits (b_r) available in the traffic in the particular instance, gathered from the particular switch, the source and destination ports (S_p, D_p) and the internet protocol address (S_{IP}, D_{Ip}) respectively. The information gathered from each device in the data layer regarding the traffic status is separately computed to identify the abnormal status of the traffic flow. The extracted information of the source IPs, destination IPs, source ports, destination ports were transformed into a quantity using Renyi's quadratic entropy concept to be utilized in the traffic status evaluation. The Eq. (1) is framed in this regard.

$$H(B) = \begin{cases} -\log \sum_{x=1}^{n} P_x, & \text{where } P_x = b_x/n \\ \text{minimal} & \text{for concentrated samples} \\ 0 & \text{for identical samples} \end{cases} \tag{1}$$

Where b_x is the probability of the occurrence of the behavior is, $B = \{\{b_1, b_2 \dots b_x\}$ is set by the behavior measured, and the extracted information on the number of the packets and bits, their quantities are assumed to be gathered when the traffic status is being collected. The traffic status is accumulated through the OpenFlow protocol [8]. This OpenFlow protocol assigns a common interface to handle the transmission of the information using the rules, settings, and configurations. Assigning the quantity to the characteristics of the traffic status would enable easy identification of the changes when subjected to the attacks. The process involved in the data accumulation is shown in Fig. 2.

3.2 DDoS Attacks Identification and Alleviation

The expected features of the traffic are used to identify the traffic into normal traffic and abnormal traffic. If traffic is normal, then packets will be forwarded. If traffic contains any abnormality means, a mitigation policy will be applied. Mitigation on the SDN environment can be obtained by applying to block or dropping or redirecting the traffic. Figure 3 illustrates DDoS attack identification and alleviation.

3.2.1 Framing of the Expected Traffic Status

The traffic status framing of the usual flow is done to distinguish between abnormal traffic status and normal traffic status. In the initial stage, the process of accumulating the traffic status, and the quantities for the features were received. Once the quantities are obtained,

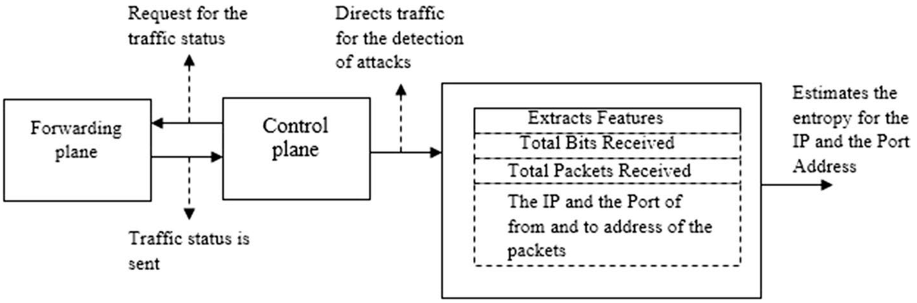

Request for the traffic status
Directs traffic for the detection of attacks
Forwarding plane
Control plane
Extracts Features
Total Bits Received
Total Packets Received
The IP and the Port of from and to address of the packets
Estimates the entropy for the IP and the Port Address
Traffic status is sent

Fig. 2 Data accumulation process

then the normal traffic status is framed by forming a cluster of the features extracted with similar quantities. The number of the clusters formed equals the number of properties excerpted. The proposed method employs the hybridized metaheuristic naturally inspired PSO-ACO [21] to frame the clusters to identify the behavior of the traffic of a particular instance. The foraging behavior of the population-based swarm intelligence of the PSO and the ACO are utilized to arrive at a global optimum. The shortest path determination using the density of the pheromone update of the ACO and the global position update procedure of the PSO enumerating the velocity and the position is clubbed in framing the cluster in the normal characteristics of the traffic. To minimize the distance between the features and the midpoint of the clusters they are grouped within. The Eq. (2) is framed in this regard.

$$Min \quad D(i,j) = \sum_{m=1}^{M} \sum_{n=1}^{N} i_{mn} \left\| \bar{j}_m - j_n \right\|^2 \tag{2}$$

where, M is the number of features (objects) and N is the number of clusters. The M features are allocated to one of the clusters in the N clusters based on the square of the Euclidean distance(ED) such that the ED between the feature and the midpoint of the cluster is placed will be minimized. Once the behavior of the traffic is framed as a cluster that holds similar features, and the differences between features of the cluster were compared. The traffic flow that is with similar characteristics of the framed clusters fit into the clusters and the traffic flow that is dissimilar to the prevailing cluster framed are considered as the

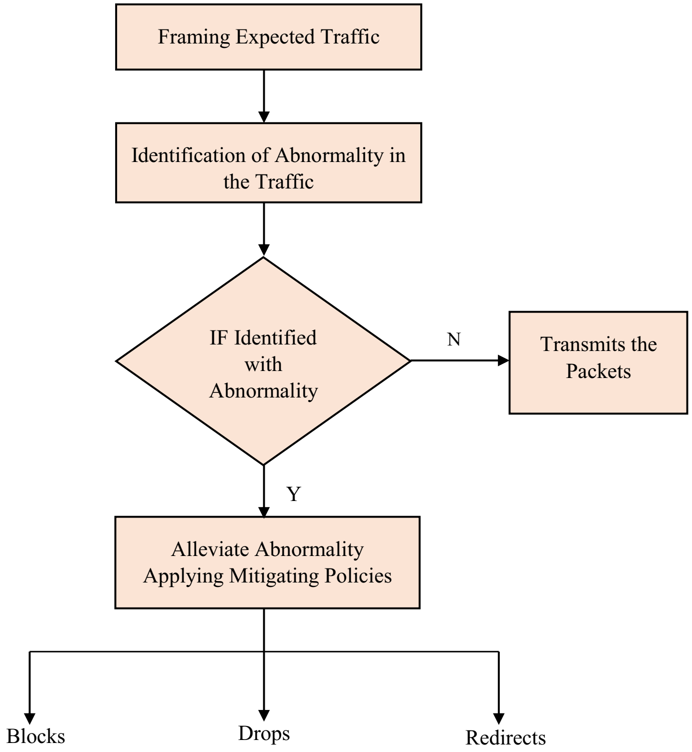

Framing Expected Traffic
Identification of Abnormality in the Traffic
IF Identified with Abnormality
N
Transmits the Packets
Y
Alleviate Abnormality Applying Mitigating Policies
Blocks
Drops
Redirects

Fig. 3 DDOS identification and alleviation

abnormal flow. It is assumed that the normal traffic status lies near the midpoint of the clusters and the traffic with the abnormal status lies at a quiet distance away from the midpoint. So the cluster that is densely packed are identified to be the normal traffic (NT) and the one that is clustered which are grouped with the smaller sizes are detected as the abnormal traffic status(AT). The Eqs. (3) and (4) is framed in this regard.

$$NT = \begin{cases} \text{distance} < \text{threshold distance} \\ \text{density} > \text{threshold density} \end{cases} \tag{3}$$

$$AT = \begin{cases} \text{distance} > \text{threshold distance} \\ \text{density} < \text{threshold distance} \end{cases} \tag{4}$$

3.2.2 Abnormal Traffic Status Identification

The traffic status acquired based on the request for the whole day is tracked and detected. The traffic status (TS) gathered for the whole day is given as $(T) = \left\{TS_1, TS_2, \ldots TS_n\right\}$, the TS acquired at the instant T based on the request is represented as (TS(T))´. The current tracked, the status of the traffic is compared with the acquired traffic of the whole day to identify the alteration or the abnormalities in the traffic.

Each characteristic extracted from the traffic status obtained is influenced by the abnormal happening that occurs, so the proposed method implements the multinomial regression method in estimating the traffic alterations that lead to the abnormalities. The multinomial regression that is the extension of the BLR with the multiple nominal outcomes, develops a classifier with the capability of segregating the traffic based on the samples used for the training. The multinomial regression here is engaged in detecting the abnormalities affecting the network operation. The traffic behavior framed as the thicker cluster used as the training data set is used in the classification of abnormal behavior. Unlike the BLR the multinomial regression allows having more number of options as shown in Table 1.

Based on the classification with one option representing the referral option. Based on the options given the dependence function (Dep_{fun}) is acquired as in the Eq. (5).

$$Dep_{fun}(Y) = \ln \left[{prob\left(Z_x = M' | Y\right)} \middle/ {prob\left(Z_x = 0 | Y\right)} \right] \tag{5}$$

where, M' represents the options, now the probability of the referral option is estimated using the Eq. (6).

$$Prob_{NT} = 1 - \sum_{M'=1}^{m} prob\left(Z_x = 0 | Y\right) e^{Dep_{fun}(Y)} \tag{6}$$

Based on the probabilityf the referral option that states the normal status the abnormal status probability ($Prob_{AT}$.) is calculated unthe eion (7).

Table 1 Categories of attack

Options	Traffic flows
0	Normal Flow
1	DDoS hulk
2	DDoS
3	BOT

$$\text{Prob}_{AT} = e^{Dep_{fun}(Y)} \Big/ 1 + \sum_{M''=1}^{m} e^{Dep_{fun}(Y)} \tag{7}$$

The relative error (R_{er}) between the $TS(T)$ and the $TS'(T)$ is obtained for the presently tracked traffic using the Eq. (8).

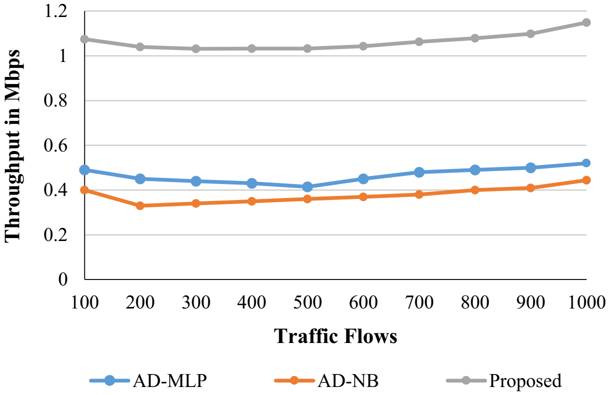
$$R_{er} = mod\big(TS(T) - TS'(T)\big) \tag{8}$$

The R_{er} enables the error calculation between the expected and ensures the identification of the abnormal flow in the SDN. Further, the interruptions in the non-malignant traffics are eluded by keeping an enrollment containing the IP and the port addresses that are set manually by the manager of the network. This enables the network to apply the alleviation procedures only if entailed. The alleviation procedures apply the mitigating techniques to evade the severity of the attacks.

3.3 Mitigation for Severity Reduction of the Attacks

The abnormal traffic status detected could harm the network by crashing the target system or stopping the services by denying them to the users. So the abnormalities detected require a certain solution to either reduce or elude the attacks directed towards the network. This is done by engaging the mitigation methods. The mitigation techniques are framed by a set of policies that react whenever it is entailed. The policy is framed based on certain conditions that are similar to the circumstance that causes the attacks. Policies are framed based on the knowledge learned from the previously occurred events (attacks) [21, 22], the mitigating policies are stored in the reserve, and the policies react automatically on requisition from the system, whenever an event occurs. Mitigating techniques respond immediately to the event and analyze them based on the previously learned events and proceeds to apply the policies once detected with the abnormalities. [23] For detection, the knowledge gained from the status, feature extracted, IP, and the port address of the abnormalities are utilized to identify the newly occurring abnormalities. The significant actions in applying the policies are as follows (i) blocks the data flow from the specific IP or the port address intimated (ii) drop the data packets that are forwarded in a particular flow, and (iii) balance the loading by redirecting the attacks to the other servers that are idle. The mitigation techniques based on the policies as shown below in Table 2 are forwarded to the switches via the controller utilizing the protocols

Fig. 4 Network throughput



(open flow) and stays active for a period of time until the abnormality detected is active. Figure 4 explains the whole process in the identification of the abnormalities and its alleviation in reducing the abnormality attacks.

3.3.1 Algorithm for DDOS Identification and Alleviation

Input: Normal and Abnormal Traffic Dump

Output: DDoS Attacks Identification and Performing Mitigation on SDN Environment

Data Accumulation Module

```
For (Time Window = T interval)
    SDN PoX Controller Request "Traffic Flow Status"
    Reply "Obtain the Current Traffic Status"
    Extracts "$S_{p,}\ D_{p,}\ S_{IP}, D_{IP,}\ S_r, D_r$"
    Enumerated Entropy "$S_{p,}\ D_{p,}\ S_{IP}, D_{IP}$" using H(B) = - $\log \sum_{x=1}^{n} P_x$
```

3.3.2 DDoS Attacks Identification and Alleviation

```
For All Traffic Flow Obtained (Framing of the Expected Traffic Status)
    $Min\ D\ (i,j) = \sum_{m=1}^{M} \sum_{n=1}^{N} i_{mn} \| \bar{J}_m - j_n \|^2$
    Normal Traffic Flow = $\begin{cases} distance < Treshold\ distance \\ density > Threshold\ Density \end{cases}$
    Abnormal Traffic Flow = $\begin{cases} distance > threshold\ distance \\ density < threshold\ Distance \end{cases}$
```

3.3.3 Abnormal Traffic Status Identification

```
Compute $TS(T)$ and $T\acute{S}(T)$
Estimate $Dep_{fun}(Y) = \ln \left[ prob(Z_x = \acute{M} \mid Y) / prob(Z_x = 0 \mid Y) \right]$
Estimate $Prob_{NT} = 1 - \sum_{\acute{M}=1}^{m} prob(Z_x = 0|Y)\ e^{Dep_{fun}(Y)}$
Estimate $Prob_{AT} = e^{Dep_{fun}(Y)} / 1 + \sum_{\acute{M}=1}^{m} e^{Dep_{fun}(Y)}$
Estimate $R_{er} = mod\ (TS(T) - T\acute{S}(T))$
```

3.3.4 Mitigation for Severity Reduction of the Attacks

```
If (Abnormality Traffic Identified)
Begin
    Block "all the traffic flow from particular address"
    Drop "the PDU for the particular address"
    Directs "the traffic flow to the utilization of fewer servers"
End
Else
    Transmit the Packet
```

Table 2 Mitigation policies and actions taken

Mitigation policies	Action taken
Blocking	Block all the traffic flow from a particular address
Dropping	Drop the PDU for the particular address
Redirecting	Directs the traffic flow to the utilization of fewer servers

So the DDoS that deteriorates the performance of the network is identified by detecting the abnormal traffic and performing the mitigation on the SDN environment. Mitigation will support the networks from reducing the severity of the attacks and protect the network from malicious flow through performing the blocking or denying or redirection.

4 Result Evaluation

The improved network is monitored through the proposed work in the SDN environment against the DDoS malicious attacks. The logical SDN is configured using a Mininet environment. Tree topology is configured in the Mininet environment. DDoS attacks are triggered to logical networks with help of hping3 utility. DDoS attack detection and the mitigating are simulated and the moment to evince its capabilities in terms of the throughput, flexible network behavior, reliability in the service provisioning, processing overhead, and the cost are considered while establishing the SDN environment. The proposed method is further compared with the prevailing method of the abnormality identification in the traffic flow, based on the varying number of traffic flows on different days, with the simulation time of 100 s in the simulation area of 2500*40 m, and the packet size of 1024 bits. Table 3 gives the simulation parameter involved.

The abnormality detection with the normal traffic framing using the ACO-PSO is and the abnormality identification employing the multinomial regression is evaluated when comparing with the other machine learning techniques such as MLP and NB used in the abnormality detection. Abnormality Detection-Multilayer Perceptron (AD-MLP) is a supervised learning approach and MLP machine learning techniques are used to detect malicious traffic. MLP comprises of 3 layer model such as input, hidden, and output, which is used to detect the DDoS malicious traffic. Abnormality Detection-Naive Bayes (AD-NB) classifiers are used to detect the malicious DDoS attacks by applying Bayes theorem. Figure 4 giving the simulation result of the throughput evaluation of the network employed with the proposed SDN techniques utilizing i) the DDoS detection techniques based on the

Table 3 Simulation parameters

Parameter	Value
Packet type	TCP/UDP/ICMP
Window size	100
Time window (Traffic Request)	30 s
Traffic flow	Up to 1000
Packets size	1024 byes

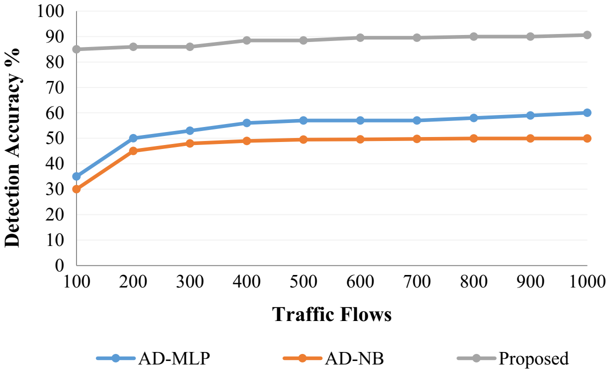


Fig. 5 Accuracy

PSO-ACO traffic characterization, ii) the multinomial regression used in the classification of the traffic, iii) the alleviation techniques mitigating the attacks by blocking the abnormal traffic flow from the particular IP addresses or the port addresses, iv) the stopping the packets of the blocked address from forwarding and enhances the throughput of the network evading the system crashes or the denial of the services to the client. The proposed method is compared with the other methods used in the classification and the characterization to identify the proficiency of the proposed.

Figure 5 shows the simulation result for the accuracy rate of the proposed method, and the expected traffic flow framed using the hybridized naturally inspired swarm intelligence enables in having a global optimum and the multinomial regression-based traffic classification. It also allows to have proper relative error between the expected and the currently tracked traffic identifying the malicious attacks. This ensures the perfect identification for the DDoS attacks. Moreover, the mitigating policies activated on the occurrence of the attacks, either drop the packets from the flow or balances the load to the other idle servers by reducing the severity of the attacks and continuing with the service provisioning without blocking or denying shows the accuracy of the proposed over the varying traffic flows. Further, they perform excellently even under the high attacks and proved to be accurate when compared to the other techniques employed for the detection.

Figure 6 shows the improved performance of the network on the varying volume of the traffic flows that have employed with the proposed method of detection and the mitigation

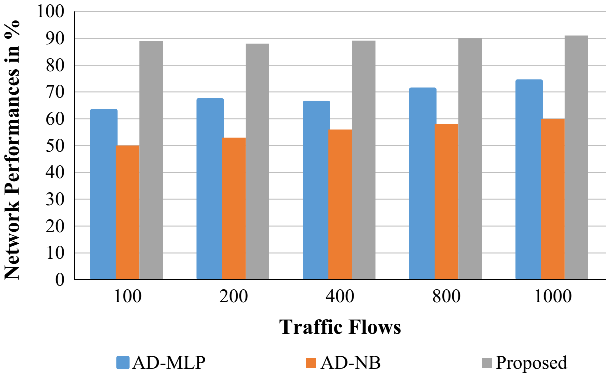


Fig. 6 Network performance

Table 4 Time utilization of the proposed method

Traffic flows	Normal	DDoS	DDoS hulk	BOT
100	0.0228	0.0895	0.0956	0.0945
200	0.0276	0.0901	0.1456	0.1654
400	0.02849	0.0954	0.1432	0.1542
800	0.02882	0.0994	0.1567	0.1632
1000	0.0289	0.0997	0.1673	0.1615

against the attacks of the DDoS that affect the performance of the system. The network always encounters a flow that includes both normal and abnormal traffic. Traffic is monitored continuously at regular short intervals by the SDN PoX controller. In the proposed method the traffic is framed for the identification of the abnormality. Further, the proceedings with the blocking of the abnormal attacks are carried by applying the policies of blocking, dropping, and redirecting are enabled by the network to have improved performance. Preventing malicious DDoS attacks improves network performance by providing secure access to resources.

Table 4 gives the simulation results on the time utilization of the proposed method using the ACO-PSO with multinomial regression. Analysis of the traffic to identify the normal traffic, and the application of the mitigation policies are observed by the result that shows the proposed method offers continuous tracking and enables the identification of the abnormal flow in the traffic along with the alleviation methods in milliseconds. The higher the intensity of the attack higher would be the time consumption of the process in identifying the abnormality and its alleviation.

Table 5 gives the abnormality identification comparison based on the precision, recall, f-measure, and the false-positive rate. The traffic flows varies for the employed multinomial regression and the other machine learning techniques MLP and the NB in which the NB is computed to have the worst performance than the other two techniques.

Table 5 shows the improvement over the precision, recall, f-measure, and the false-positive rate. Thus the proposed method enables in identifying the abnormality in the traffic by applying the natural-inspired and the machine learning techniques, this leads to an improvement for monitoring the network at regular short intervals. Further utilizes the policies of the mitigation with the action of the blocking, redirecting, and dropping to reduce the severity of the attacks or block the attacks from crashing the network causing the DDoS.

5 Conclusion

The SDN, which regulates the network traffic properly, by separating the forwarding and the control plane and also enables the network configuration easily, and the migration of the network new protocols paves the way for the network to have improved efficiency. Despite all these merits the SDN controlled network often suffers from the DDoS attacks caused by a multitude of the compromised systems that affect the network. This article addresses the problem of the attacks caused by the DDoS in the network proceeds as three stages one accumulation of the traffic data to track the details of the traffic flow, then with the abnormal traffic identification the further proceeds a stage

Table 5 Comparison of abnormality identification

Traffic flows	AD-NB				AD-MLP				Proposed method			
	Precision	Recall	F measure	False positive	Precision	Recall	F measure	False positive	Precision	Recall	F measure	False positive
100	75	65	57	30	82	68	65	15	85	74	70	7
200	75.4	68	54	45	84	70	62	10	88	75	71	5
400	76	63	58	47	85	75	66	13	88.5	76.8	72	4
800	74.2	64	53	40	85.3	73	63	11	90	79.2	75	6
1000	74	63	54	41	86.1	74	64	9	90.2	79.8	76	4

two with the characterization (framing) of the traffic using the ACO-PSO and the identification of the abnormalities in the traffic using the multinomial regression methods and finally the stage three with the alleviation for the DDoS as mitigation policies with blocking, redirecting and dropping to reduce the severity of the attacks. Further, the proposed method is validated using the Mininet to show the capabilities of the proposed method in improving the network performance when compared to the other methods. In the future, this research can be is proceeded with the analysis of the novel detection techniques employing other Machine Learning methods in the identification of the DDoS of high and low rates.

References

1. Hu, F., Hao, Q., & Bao, K. (2014). A survey on software-defined network and openflow: From concept to implementation. *IEEE Communications Surveys & Tutorials, 16*(4), 2181–2206.
2. Nunes, B. A. A., Mendonca, M., Nguyen, X.-N., Obraczka, K., & Turletti, T. (2014). A survey of software-defined networking: Past, present, and future of programmable networks. *IEEE Communications Surveys & Tutorials, 16*(3), 1617–1634.
3. Smys, S. (2019). DDOS attack detection in telecommunication network using machine learning. *Journal of Ubiquitous Computing and Communication Technologies (UCCT), 1*(01), 33–44.
4. Van Adrichem, Niels, L.M., Christian D., and Kuipers, F.A. (2018) Opennetmon: Network monitoring in openflow software-defined networks." In *2014 IEEE Network Operations and Management Symposium (NOMS)*, pp. 1–8. IEEE.
5. Kim, H., & Feamster, N. (2013). Improving network management with software defined networking. *IEEE Communications Magazine, 51*(2), 114–119.
6. Luo, T., Hwee-Pink, T., & Quek, T. Q. S. (2012). Sensor OpenFlow: Enabling software-defined wireless sensor networks. *IEEE Communications Letters, 16*(11), 1896–1899.
7. Mugunthan, S. R. (2019). Soft computing based autonomous low rate DDOS attack detection and security for cloud computing. *Journal of Soft Computing. Paradig. (JSCP), 1*(02), 80–90.
8. Li, W., Weizhi, M., & Lam, F. K. (2016). A survey on OpenFlow-based Software Defined Networks: Security challenges and countermeasures. *Journal of Network and Computer Applications, 68,* 126–139.
9. Pakzad, F., Marius, P., Wee, L. T., & Jadwiga, I. (2016). Efficient topology discovery in OpenFlow-based software defined networks. *Computer Communications, 77,* 52–61.
10. Akyildiz, I. F., Ahyoung Lee, P., Wang, M. L., & Chou, W. (2016). Research challenges for traffic engineering in software defined networks. *IEEE Network, 30*(3), 52–58.
11. Smys, S., Abul, B., & Haoxiang, W. (2020). Hybrid Intrusion Detection System for Internet of Things (IoT). *Journal of ISMAC, 2*(04), 190–199.
12. Rai, Sandesh, Kalpana Sharma, and Dependra Dhakal. "A Survey on Detection and Mitigation of Distributed Denial-of-Service Attack in Named Data Networking." In *Advances in Communication, Cloud, and Big Data*, pp. 163-171. Springer, Singapore, 2019.
13. Rai, S., and Dependra D. (2018) A survey on detection and mitigation of interest flooding attack in named data networking. In *Advanced Computational and Communication Paradigms*, pp. 523–531. Springer, Singapore
14. Rao, N. Srihari, Chandra Sekharaiah, K., and Ananda Rao, A., (2019). A survey of distributed denial-of-service (DDoS) defense techniques in ISP domains." In *Innovations in Computer Science and Engineering*, pp. 221-230. Springer, Singapore
15. Shakya, S. (2020). Process Mining Error Detection for Securing the IoT System. *Journal of ISMAC, 2*(03), 147–153.
16. Carl, G., Kesidis, G., Brooks, R. R., & Rai, S. (2006). Denial-of-service attack-detection techniques. *IEEE Internet Computing, 10*(1), 82–89.
17. Yan, Q., Richard Y u, F., Qingxiang, G., & Jianqiang, L. (2015). Software-defined networking (SDN) and distributed denial of service (DDoS) attacks in cloud computing environments: A survey, some research issues, and challenges. *IEEE Communications Surveys & Tutorials, 18*(1), 602–622.
18. Ahmed, M., Abdun, N. M., & Jiankun, H. (2016). A survey of network anomaly detection techniques. *Journal of Network and Computer Applications, 60,* 19–31.
19. Bawany, N. Z., Jawwad, A. S., & Khaled, S. (2017). DDoS attack detection and mitigation using SDN: methods, practices, and solutions. *Arabian Journal for Science and Engineering, 42*(2), 425–441.

20. Yan, Q., Wenyao, H., Xupeng, L., Qingxiang, G., & Richard, F. (2018). A multi-level DDoS mitigation framework for the industrial internet of things. *IEEE Communications Magazine, 56*(2), 30–36.
21. Marinakis, Y., Marinaki, M., & Matsatsinis, N. (2008). A stochastic nature inspired metaheuristic for clustering analysis. *International Journal of Business Intelligence and Data Mining, 3*(1), 30–44.
22. Haoxiang, W., & Smys, S. (2020). Secure and Optimized Cloud-Based Cyber-Physical Systems with Memory-Aware Scheduling Scheme. *Journal of trends in Computer Science and Smart technology (TCSST), 2*(03), 141–147.
23. Han, W., & Lei, C. (2012). A survey on policy languages in network and security management. *Computer Networks, 56*(1), 477–489.
24. Krishnaraj, N., & Smys, S. (2019). A multihoming ACO-MDV routing for maximum power efficiency in an IoT environment. *Wireless Personal Communications, Springer, 109*(1), 243–256.
25. Seethalakshmi, V., & Mohan Kumar, G., (2014). Fuzzy analysis and Performance Evaluation of QoS based Routing in MANET", *Journal of Electrical Engineering*, 14(3), Article 14.3.3, 1–10.
26. Seethalakshmi, V., & Mohan Kumar, G., (2014). Analysis of QoS based Routing Algorithm in MANET Using Fuzzy logic. In *International Journal of Computing and Digital Systems, Scientific Publishing Center, University of Bahrain*, Vol. 3, No. 2, pp. 111–122.
27. Ramprakash, P., Sakthivadivel, M., Krishnaraj, N., & Ramprasath, J. (2014). Host-based Intrusion Detection System using Sequence of System Calls. *International Journal of Engineering and Management Research, Vandana Publications, 4*(2), 241–247.
28. Ramprasath, J., & Seethalakshmi, V. (2021). Secure access of resources in software-defined networks using dynamic access control list. *International Journal of Communication Systems, 34,* e4607. https://doi.org/10.1002/dac.4607.

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

J. Ramprasath, working as an Assistant Professor in the Department of Information Technology at Dr. Mahalingam College of Engineering and Technology, Pollachi, India. He has done his B.Tech in Information Technology from Dr. Mahalingam College of Engineering and Technology, Pollachi, India. M.E in Computer Science and Engineering from V.L.B. Janakiammal College of Engineering and Technology, Coimbatore, India. He pursues Ph.D. in Information and Communication Engineering from Anna University, Chennai, Tamil Nadu, India. His research interests are in Computer Networks, and Software Defined Networking. He has 9 years of teaching experience. He has presented 6 papers in conferences and also he published 3 papers in the international journal.

Dr. V. Seethalakshmi, working as an Associate Professor in the Department of Electronics and Communication Engineering at KPR Institute of Engineering and Technology, Coimbatore, India. She has completed her B.E in Electrical and Electronics Engineering from PSG College of Technology, Coimbatore, India. M.Tech in Electronics and Communication Engineering from PTU University, Punjab, India. Ph.D. in Information and Communication Engineering from Anna University, Chennai, Tamil Nadu, India. Her research interest is on Network Routing, Computer Networks, Wireless Sensor Networks, Vehicular Adhoc Networks, and Embedded Systems. She has 23 years of experience in the industry as well as teaching. She has presented 25 papers in National Conference and 24 papers in the International Conferences. She has also published 28 papers in international journal and published 5 books.