Classification and Prediction of traffic in Optical Burst Switched Networks using Machine Learning

Deepali Bhawarthi, Dr .Girish Chowdhary

[1]*Research Scholar, Shri Guru Govind Singhji, IE&T, Nanded, Maharashtra, India*

[2]*Professor and Director, School of Computational Sciences, Nanded, Maharashtra, India*
[1]*dipali.bhawarthi@gmail.com*,[2]*girish.chowdhary@gmail.com*

Abstract

Optical burst switched (OBS) networks has been emerged as a new infrastructure of this century for optical internet. The classification of network traffic and segregation of normal traffic from the malicious traffic is vital for security and data integrity in OBS. The traffic classification mechanism should be dynamic and capable enough to segregate the network traffic in a quick manner, so that the malicious traffic is identified, then deflected at the early stage and the normal traffic is to be channelized to the destined nodes. In this paper, we are presenting two phased machine learning based mechanism. The first phase focuses on the segregation of network traffic into four different classes which assist in reducing the congestion over channels, enhancing the network throughput and providing secure services to end users. The second phase is providing insights into the prediction of traffic load using convolutional neural networks for channelization of the normal traffic over under-utilized and least loaded channels.

Keywords: *Optical Burst Switched Networks, Convolutional Neural Network, Congestion, Machine Learning.*

1. Introduction

In recent years, the demand for network bandwidth has increased at a rapid rate. It is considered to be a major challenge for high-speed networks due to increase in user Apps and popularity of Internet. The efforts are being made worldwide to provide network bandwidth of high capacities to the users at a minimum cost. Optical data communication has offered optimum solution to suffice the demand of users by providing high bandwidth and by supporting various network services [1], [2]. OBS is a new technique that attempts to resolve the problem of allocation of computational resources for bursty internet traffic [3]. OBS offers combine features of the fine grained packet switching and coarse grained circuit switching paradigms. OBS handles bursty traffic efficiently generated by the networks.

An OBS switch is made of optical and electronic components which include multiplexers, de-multiplexers, an optical switching network, an input module, an output module; a control burst router and a scheduler. OBS uses two planes: the control plane and the data plane. Data packets are clubbed into larger bursts before transmitting over the network. The control burst requests for allocation of resources at each switch. The data burst is sent on a separate wavelength. At each intermediate node, the control burst is processed electronically. The time taken for processing a control burst is called as processing time. The control burst then reserves bandwidth on an outgoing channel for the upcoming data burst. The reservation period is the period between the arrival of the data burst and the completion of the data burst transmission. The usage of OBS communication technology has resulted into many critical issues such as traffic load balancing, channelization of network traffic, task sharing in numerous devices, responsiveness and throughput [4], [5], and [6].

OBS networks are getting much attention as a promising infrastructure to construct next level optical Internet. In order to provide Quality of Services (QoS) to real time traffic in OBS networks it is necessary to classify the network traffic and to channelize the normal traffic in an appropriate manner. We have attempted to propose two phased mechanism for segregating the traffic using machine learning and to predict traffic load on OBS channels using deep neural networks to make OBS an infrastructure of next generation optical Internet. Machine learning techniques provide solutions to the real world complex problems. In first phase, the ability of machine learning (ML) techniques are exploited for classification of bursty traffic .In second phase, convolution neural network (ConvNet) is proposed to predict the traffic load and for utilizing the links according to the predicted load. The contribution of the research work can be observed in both the proposed phases. In first phase, we have modified the XGBoost classifier and Bagging classifier to optimize the accuracy of classification techniques in order to segregate the blocked and malicious traffic from the normal traffic. In second phase, we have proposed our own deep ConvNet for predicting the traffic load to utilize the links/channels optimally for forwarding the traffic.

This research paper is structured into four sections. First section of the paper provides background detail and introduction of OBS network and advantage of using dynamic machine learning algorithms to classify the network traffic and prediction of traffic load. The second section provides insights into the existing techniques for classifying network traffic. The third section elaborates the proposed machine learning and deep learning based techniques. The fourth section of this paper concludes our work and also provides future directions in the area of our research work.

2. Related Works

Nowadays the usage of OBS based networks is increasing in a fast manner and the researchers around the world are putting efforts to find innovative solutions for the deployment of services over OBS [7]. OBS requires the connected devices to be accessed and controlled remotely .Traffic classification is vital for OBS enabled networks to prioritize the traffic for various reasons such as QoS services to users, detection of malicious traffic and to channelize the normal traffic. Many innovative techniques have been proposed by the researchers for classifying the network traffic [8], [9], [10], [11], [12], [13], [14], [15] and [16] but OBS needs more dynamic approaches to classify the huge traffic and predicting the traffic load. We have explored the existing techniques prior to elaborating our research work in this section of the paper. The oldest and the most common technique to identify the traffic is port number based traffic classification. TCP and UDP packet headers are used to get the information about port numbers and the classification is made accordingly by making comparison between the assigned TCP or UDP port numbers [17], [18]. There are other state-of-the-art approaches such as Payload based classification. In many applications, the packet information is used to classify the traffic [19]. The payload based techniques are presented by [20], [21] and [22] for the classification of the traffic. However, payload based techniques avoid dependency on port number based classification but these techniques are also incapable in dealing with encrypted traffic.

2.1 Machine learning based approaches

In [23], authors proposed Bayesian neural network (BNN) to identify P2P protocols such as Kazaa, Bit Torrent and GnuTella and achieved good accuracy. In [24], the authors made use of DHTCP to collect traffic samples. Then neural network based approach was applied to classify the Web and P2P based traffic. In [25], a KSOM (Kernel-Self-Organizing Maps) method was used to determine the matching degree between the connection weight and the input patterns. KSOM attained better precision in comparison to Self-Organizing Maps. In [26], authors studied the flow-based features to identify VPN traffic and to segregate the traffic into different classes by using k-NN and C4.5 algorithm and the classification was made for Web browsing, streaming, file transfer, email, chat, and VoIP categories. Their research outcome achieved 92% sensitivity score using k-NN technique and 88% using C4.5. In [27], an attempt was made to classify the traffic at applications layer considering Facebook, Twitter, Skype and many others applications. The machine learning techniques such as Random Forest, Bayes Net, J48 and k-NN were used. The result outcome stated that k-NN and Random Forests gave better accuracy of 93.94% and 90.87% respectively.

2.2 Traffic and channel prediction Techniques

The channel prediction methods consume the information present in the application layer of packets [19]. The traffic load is predicted and the traffic is channelized over less utilized channels. The works presented in [28], [29], [30], [31], [32],[33] and [34] are based on effective routing based on traffic load and sensing of channels. On the basis of historical information, the future load on the network links is determined and traffic is directed accordingly. Though there exist many approaches to classify the network traffic and predicting the traffic load but with the advent of OBS, the classification of traffic cannot be made using static algorithms. There is a need to explore newer algorithms which are capable enough to segregate the dynamic traffic in OBS networks to handle congestion control, to improve network throughput and to utilize the channels optimally. Hence, we are proposing dynamic machine learning based approaches to classify the traffic and channelize the traffic.

3. Proposed Approach

The traffic over OBS enabled networks is increasing rapidly due to the advent of new applications, technologies and software’s. It is important to address the user needs to provide them QoS (quality of service) seamlessly. The machine learning based methodologies help to provide QoS based services to users by segregating the normal traffic from the malicious traffic to avoid network congestion and to enhance the network throughput. In this paper, we are experimenting machine learning methods to segregate the network traffic in an accurate manner so that the unwanted traffic can be blocked and the normal traffic can utilize the channel optimally. Accurate classification of the traffic at access points allows efficient allocation of resources to users to ensure QoS. We have classified the traffic into 4 classes as Malicious, Normal, Non Behaving and traffic in queue. By using machine learning, we can automatically identify the affected nodes and then we can free up the resources which will increase the network bandwidth automatically. We can also find out the trends and patterns of the flood attacks and use it for early detection of flood attack or a malicious attack.

3.1 Attributes considered for machine learning based approach

The attributes considered for the research study are shown in Table 1.

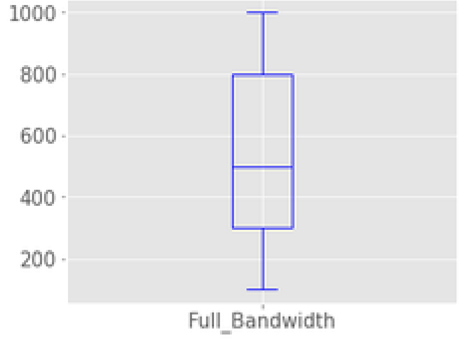
Table 1: Parameters considered for classification of the traffic

Sr. No	Attribute	Description
1.	Utilized Bandwidth Rate	This field provides info on used Bandwidth
2.	Node	It specifies the active nodes able to send data
3.	Packet drop rate	This field provides information on lost-packet rate in percentage
4.	Reserved Bandwidth	Specifies the bandwidth allocated to each node
5.	Avg delay time	It specifies the delay time
6.	% of lost packet rate	It tells the rate of the packets lost during transmission
7.	% of lost byte rate	specifies the rate of the Bytes lost during transmission
8.	Packets receivable rate	No. of packets received each second by the nodes
9.	Used bandwidth	Specifies the consumption of bandwidth
10.	Lost Bandwidth	Depicts lost bandwidth out of the reserved one
11.	Packet size byte	represents the size of Packet in Byte
12.	Packets Transmitted	Represents packets transmitted each second for all nodes
13.	Packets Received	Represents no. of packets received each second
14.	Packets lost	Represents total no. of lost packets per second
15.	Transmitted bytes	Total no. of bytes transmitted per second
16.	Received Byte	Total bytes received per Second
17.	10 Run Avg drop rate	Avg packet drop rate for 10 runs
18.	10 Run Avg bandwidth	Avg bandwidth utilized for 10 runs
19.	10 Run delay	Avg latency time for 10 runs
20.	Node status	Classifies the Nodes
21.	Burst Loss	It tells the burst loss
22.	Throughput	Specifies the throughput of OBS network

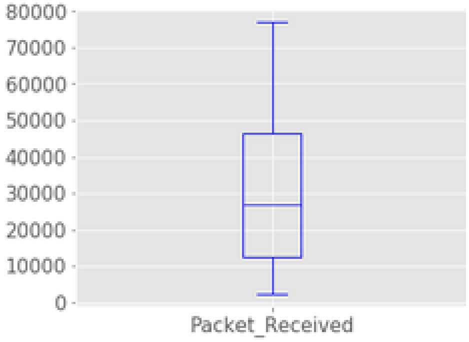
The proposed machine learning based classification mechanism begins with the data collection and data visualization. We are making use of data visualizations before applying machine learning based classifiers for better understanding of readers.

3.2 Whisker or Box Plots:

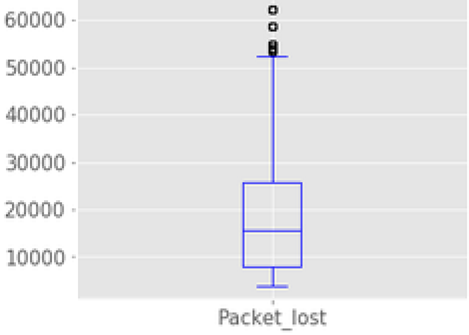
The whisker plot depicts the distribution of data from the first quartile. It shows whether the data has normal distribution or not. The box plots go from each quartile to the maximum or minimum. The Box plots for full bandwidth, utilized bandwidth, packet received, packet received rate, packets transmitted and packets lost, Transmitted bytes and Received bytes are shown in Figure.1 (a-h). We can conclude from the Box plots that the data is not uniformly distributed and the data is mostly skewed. We need normally distributed data while applying machine learning algorithms. Hence, we have applied rescaling methods on the dataset for making it usable for our machine learning based classification approaches. After balancing the dataset, we have applied machine learning based techniques to classify the traffic into 4 classes as explained in next subsection of this paper.



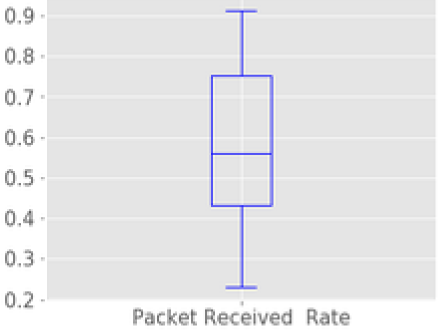
a) Box Plot for Full Bandwidth



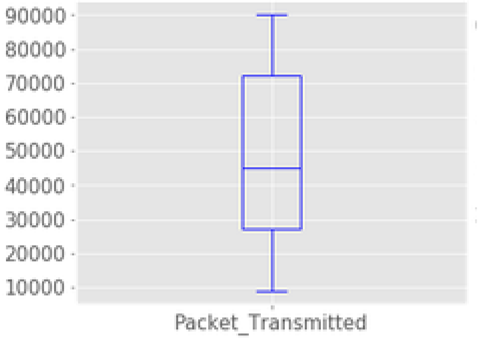
b) Box Plot for Packet Received



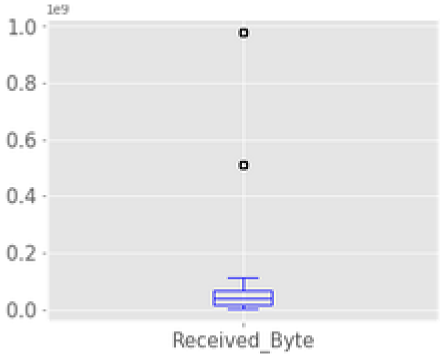
c) Box Plot for Packet Lost



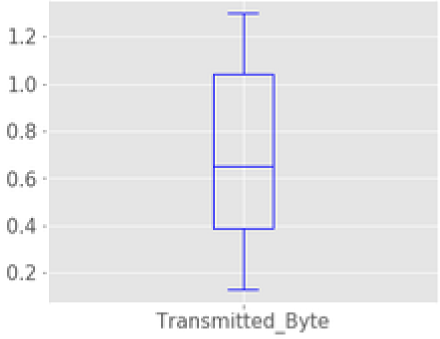
d) Box Plot for Packet Received Rate



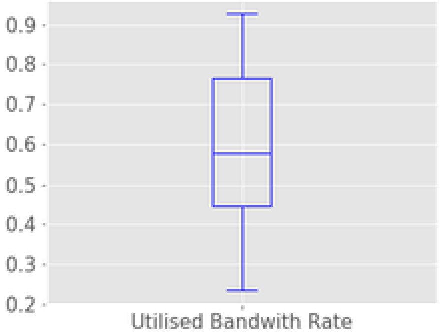
e) Box Plot for Packet Transmitted



f) Box Plot for Received Byte



g) Box Plot for Transmitted Byte



h) Box Plot for Utilized Bandwidth Rate

Figure 1: Box Plot/Whisker Plot

3.3 Phase I-Traffic classification using Machine learning methods

The machine learning based algorithms such as XGBoost and Bagging classifier have been implemented with modifications with respect to our problem statement. The network traffic is classified into 4 classes, NB-No Block consists of non-behaving traffic, Block consists of blocked nodes, No-Block comprises Normal node or Working Node, NB-Wait comprises waiting nodes due to many processes or bursty traffic. Our aim is to free up the congestion by removing non behaving nodes and blocked nodes and to channelize the normal traffic by predicting the free and appropriate OBS channels. The performance of each algorithm is evaluated by using the parameters such as confusion matrix, classification accuracy score, sensitivity score, and receiver operating characteristic (ROC) Curve and F1 Score.

3.3.1 XGBoost Classifier: XGBoost is also known as ensemble learning technique [36], [37].XGBoost is a robust machine learning algorithm which dominates structured datasets on predictive modeling problems and classification. The implementation of XGBoost has been engineered for improving the efficiency of memory resources and computational time. XGBoost makes use of memory efficiently by learning fast through parallel and distributed computing (PDC). There are circumstances when it may not be sufficient to rely upon the outcomes of just one machine learning method. In those cases, ensemble learning with XGBoost provides a better solution by integrating the predictive or classification power of multiple learners. The resultant outcome is a single model that gives aggregated output. XGBoost implementation features comprises as follows in our research study:

1. Sparse aware execution with handling of missing data values in an automated fashion.
2. Block structure for supporting parallelization of the decision tree construction.
3. Continued training for further boosting of existing fitted model on new data.
4. An additive model has been integrated to add weak learners for minimizing the loss function.
5. New weak learners have been added to rectify the residual errors of existing trees.

The result is a powerful predictive modeling algorithm. The evaluation of the proposed algorithm is represented using confusion matrix in Figure. 2, Figure 3 shows ROC curve and performance matrix is shown in Table 2.

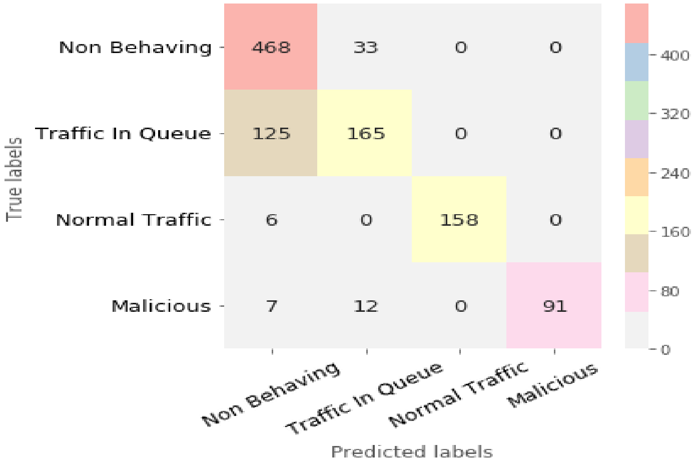


Figure 2: Confusion matrix

Table 2: Performance Matrix

Type of Traffic	F1 Score	Precision	Recall
Non Behaving	0.88	0.87	0.8
Traffic in Queue	0.68	0.75	0.62
Normal	0.98	0.98	0.98
Malicious	0.96	0.94	0.97

Following are the observations from the confusion matrix:
• In testing dataset, there are total 501 records having the target variable 185 as 'Non Behaving' and 468 records have been correctly predicted and 33are misclassified.
• In testing dataset, there are total 290 records having the target variable as 'Traffic in Queue'. 165 records have been correctly predicted and other 125 are misclassified.
• There are total 164 records having 'Normal Traffic' as the target variable. 158 records have correctly predicted and other 6 have been misclassified.
• There are total 110 records with 'Malicious' as the target variable in the testing dataset. 91 records have been predicted correctly and remaining 19 have been misclassified

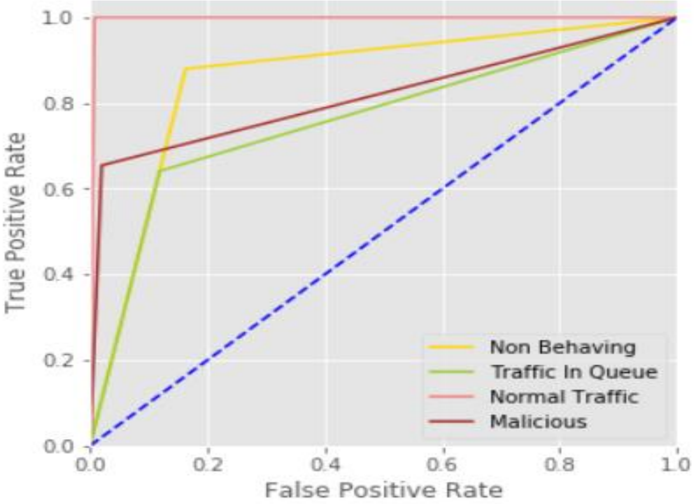


Figure 3: ROC curve for XGBoost

3.3.2 Bagging Classifier: Bagging Classifier also belongs to a family of machine learning based ensemble algorithms [38]. In bagging technique, numerous decision trees are generated simultaneously that creates base learners for the model. The outcome generated from all the base learners is aggregated. Initially we have used CART (classification and regression trees) method to generate the decision trees. Since the decision trees exhibit sensitivity w.r.t the trained data. In case, the training data is changed, the resulting tree could be fairly unique and the resultant outcome could be utmost different. Bagging algorithm using CART would work as follows.
• We have created many random subsamples of dataset
• The CART system is trained for each subsample.
• For testing, the average outcome of each CART system is determined.
• The proposed learning algorithm has put limit to a random sample of attributes to search. The number of attributes searched for are:

$ra = sqrt(vr),$

Where ra is the no. of randomly identified attributes that can be searched and vr represents the input variable. The performance of bagging model is represented by confusion matrix (Figure. 4), ROC curve (Figure. 5) and evaluation matrix as shown in

Table 3.
Following are the observations from Figure.4:

- In testing dataset, there are total 501 records having the target variable as 'Non Behaving' and 475 records were correctly predicted and 26 were misclassified.
- In testing dataset, there are total 290 records having the target variable as 'Traffic in Queue'. 242 records were correctly predicted and other 48 are misclassified

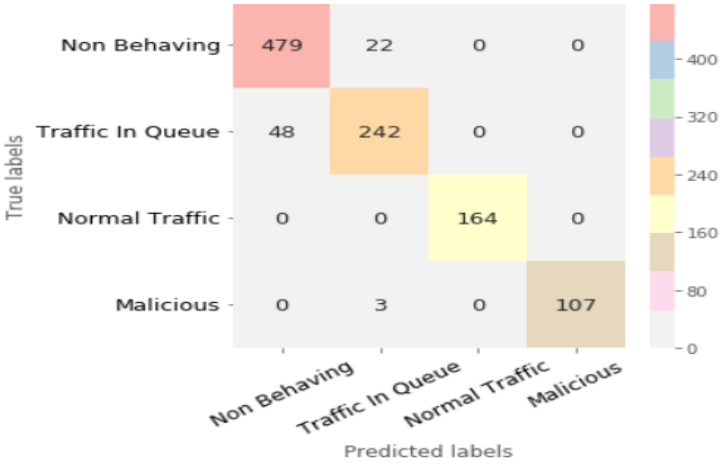


Figure 4: Confusion matrix for Bagging model

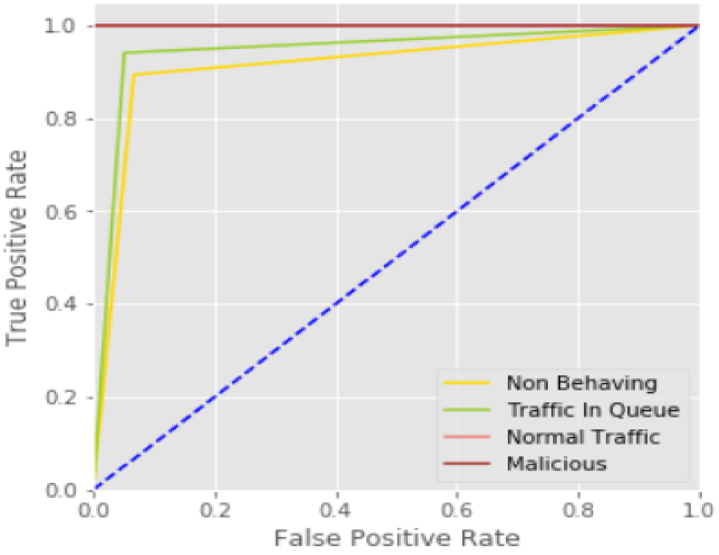


Figure 5: ROC curve for Bagging Classifier

There are total 164 records having 'Normal Traffic' as the target variable and all are correctly predicted.

- There are total 110 records with 'Malicious' as the target variable in the testing dataset. 107 records have been predicted correctly and remaining 3 has been misclassified.

Table 3: Performance matrix for Bagging Classifier

Type of Traffic	F1 Score	Precision	Recall
Non Behaving	0.91	0.92	0.89
Traffic in Queue	0.91	0.87	0.94

Normal	0.99	0.98	0.98
Malicious	0.99	0.98	0.98

We have made use of the most powerful methods of machine learning to classify the traffic on OBS networks to minimize congestion, to segregate the malicious traffic from the normal traffic, and to maximize the network throughput. We have presented the overall comparison of the performance of the algorithms considered for our study in Table 4.

Table 4: A matrix presenting the performance of the ML based classifiers

Algorithms	Training Accuracy	Test Accuracy	F1 Score	Precision	Sensitivity
XGBoost Classifier	81.9%	87.0%	86.02%	85.45%	0.87
Bagging Classifier	91.9%	88.0%	93.02%	93.0%	0.93

It is observed from the results presented in Table 4 that the modified Bagging classifier produces the most accurate results, XGBoost based classifier is next to Bagging approach in classifying the traffic accurately on OBS networks. The accurate classification over normal, non-behaving and malicious data is the need of the hour to provide seamless services to the users without any interruption. The data in OBS based networking environment is huge and it is essential to block the malicious data by classifying at the early stages. The normal traffic are also of different types such as in waiting condition and in flowing condition and can be prioritized. Hence, we have classified the normal traffic into two classes. The static techniques are not sufficient enough to fulfill the on demand services of OBS networks by classifying the data at certain intervals. The ML based algorithms facilitate in classifying the traffic dynamically and enhances the transmission rate by reducing congestion as shown in Figure. 6.It also provides security to data by deflecting the malicious data. The timely classification certainly provides solution to reduce the congestion and to forward the normal traffic to the intended nodes. After classifying the traffic, the malicious traffic could be deflected and non-behaving traffic is also blocked, so that normal traffic can move in a fast manner among the optical burst switches. We have also attempted to make use of deep neural networks to predict the traffic load and channel utilization for forwarding the normal traffic to the intended nodes.

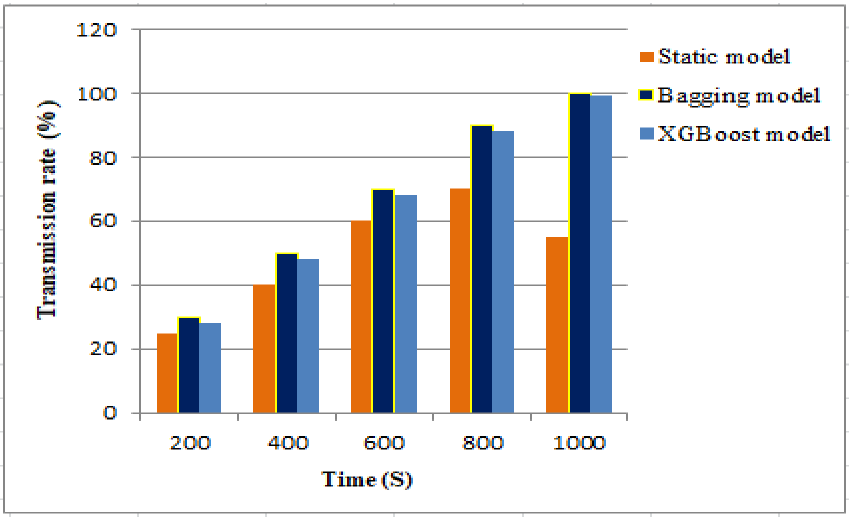


Figure 6: Transmission rate after segregation of traffic

4. Phase II-Prediction of traffic load using ConvNet

The previous section elaborates the classification mechanism. Once the traffic is classified, malicious traffic is quarantined and normal traffic can be forwarded to the designated nodes. This section explains the ConvNet (convolutional neural networks) based traffic load forecasting mechanism. The proposed technique not only predicts the traffic but can also be extended for appropriate channel assignment to the end users. The conventional algorithms focus on the current traffic load but in real time scenario, the traffic pattern can be changed any time due to sudden or bursty data in OBS based networking environment. The prediction of traffic load is very essential in OBS networks because the incorrect assignment of network link wastes the bandwidth, and also impact the network throughput negatively. Hence, we are proposing a novel deep neural network based intelligent traffic load prediction mechanism to ascertain the incoming network traffic.

For prediction of traffic load, each smart switch collects the information of the nodes that are communicating through that channel. The switches gather and forward the updated training data to the central controller over OBS networks. At each step, switches gather the network data and forward it to the controller. The load of all switches is aggregated by the controller. The proposed ConvNet based model keeps on learning from the incoming data at central controller as a decimal vector and train itself. The proposed model invokes the update function periodically during the packet transmission process. After invoking the function iteratively, an appropriate amount of data is gathered for training the ConvNet based prediction module. Due to heavy traffic load on the OBS enabled network, it is not advisable to deploy only one neural network to train and update all the switches simultaneously. Hence, numerous neural networks are integrated to make the computational tasks easy; each neural network is deployed on each switch. The training weighting matrix for each switch is represented as:

$$WS_{i}\ j \mid i \leq S, j \leq L_{max}$$

Where S represents the no. of switches and Lmax quantifies the maximum no. of channels connected to each switch. The network traffic load ntl_i^s in time slice i on switch s can be represented as: $ntl_i{}_i^s = ntl_i^1, ntl_i^2, \ldots, ntl_i^s$.

The attribute considered for research study are spatial distribution, temporal distribution, message transfer time, processor utilization, channel waiting time, network response time, channel utilization and input waiting time. The spatial and temporal distributions assist in quantifying the traffic workloads. The channel utilization provides information whether the channel is free or busy before transmission of packets. For training the ConvNet, a standard dataset available at UCI [35] machine learning repository is used and 30% of data is used for testing purpose whereas 70% data is used for training the ConvNet. The experimental setup is made on PARAM SHAVAK 'Supercomputing in a Box', which has been designed for simulation based research purposes using deep neural networks. We have made use of JNetworkSim, a Network Simulator written in Java and developed by Stanford University. Our proposed ConvNet system operates in two steps, i.e. training phase and running phase. The fine tuning of parameters is stated in Table 5.

Table 5: The parameter values of ConvNet based model for traffic prediction

Attributes	Fine-tuned values
ConvNet Layers	2
Fully-connected Layers	2
Pooling Layers	0
Packet Size	1kb
Link Bandwidth	240 Mb/s
Time interval	1s
Retraining time interval	100s
Input units	16
Output units	16

The evaluation of the proposed deep ConvNet is measured by using root mean square error as shown in Table 6, by r-squared values as shown in Figure 7 and predicted v/s actual channel utilization is shown in Figure 8. It is observed from the results that the ConvNet based predictor produces accurate results, for predicting the traffic load on OBS defined networks and assists in assigning the free channels to the traffic by predicting future load of traffic on the links. It also enhances the network throughput as shown in Figure 9. The accurate prediction of traffic load and its effective channelization is the need of the hour to provide seamless services to the users without any interruption. We have tried to achieve accurate classification of traffic and load of traffic on OBS defined networks for improving transmission rates and network throughput.

Table 6: Root mean square error analysis for ConvNet prediction model

Sr. No	Switches	RMSE
1	9	0.14
2	16	0.39
3	25	0.52
4	36	0.67
5	49	0.78
6	364	0.92

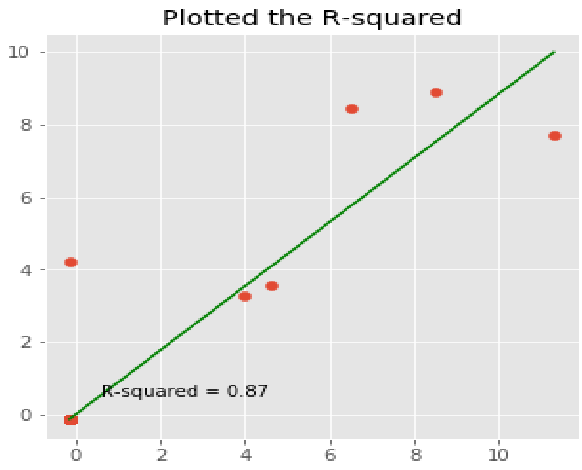


Figure 7: Chart for R-squared value

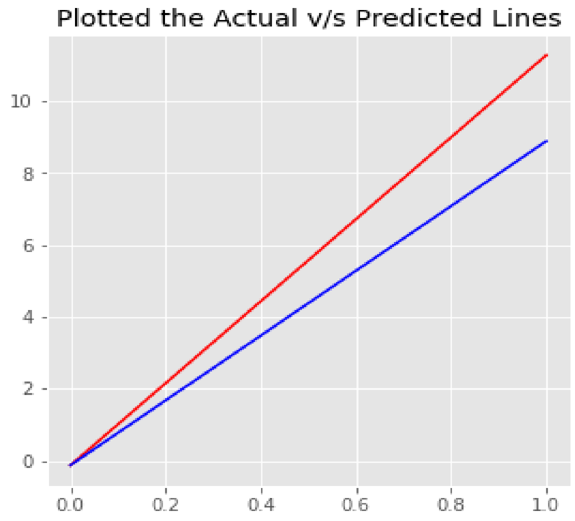


Figure 8: Chart for predicted v/s actual traffic load

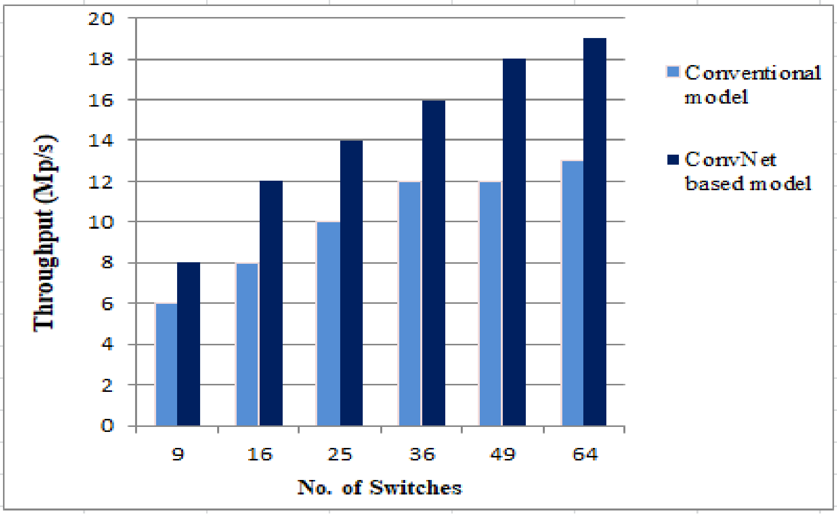


Figure 8: Throughput of the OBS network with ConvNet based model

Conclusion

Optical Burst switched networks are gathering huge sensing data each second and are expected to respond quickly in order to provide seamless services to the users. In OBS networks, high-speed transmission is attracting uttermost importance .However, OBS networks have improved the transmission tremendously but looking attentively at the high computational needs of users, we have proposed machine learning based methods for classifying the network traffic over OBS networking environment. First of all, we have classified the network traffic into 4 classes using machine learning approaches. The motive behind classification of traffic is to segregate the normal traffic from the malicious traffic, so that the malicious traffic can be blocked at the earliest and normal traffic should be forwarded to the intended nodes. We have evaluated the performance of machine learning algorithms using performance matrices such as accuracy score, F1 score, confusion matrix, precision and recall matrices. The high dynamics of traffic loads on OBS networks give rise to need for using dynamic algorithms and we have attempted to serve the requirement of the OBS networks by providing machine learning based classification methods and deep learning based traffic load prediction for channelizing the traffic according to the priorities of the traffic defined by OBS protocols

References:

[1] G. Zeng, A review on a new conservation law in optical burst switching networks, Mathematical and Computer Modelling 57 (5) (2013) 1504 - 1513.

[2] A. Detti, V. Eramo, M. Listanti, Performance evaluation of a new technique for IP support in a WDM optical network: optical composite burst switching (ocbs), Journal of Lightwave Technology 20 (2) (2002) 154-165.

[3] M. Z. Hasan, K. Z. Hasan, A. Sattar, Burst header packet ood detection in optical burst switching network using deep learning model, Procedia Computer Science 143 (2018) 970 - 977, 8th Int. Conf. on Adv. in Computing and Communications (ICACC2018).

[4] S. Verma, H. Chaskar, R. Ravikanth, Optical burst switching: A viable solution for terabit ip backbone, in: IEEE Networks, 2000, pp. 48-53.

[5] P. K. Chandra, A. K. Turuk, B. Sahoo, Survey on optical burst switching in wdm networks, in: 2009 Int. Conf. on Indust. and Info. Systems (ICIIS), 2009, pp. 83-88.

[6] A. Jenefa, M. B. Moses, Multi level statistical classi_cation of network traffic, in: 2017 Int. Conf. on Inventive Comp. and Informatics (ICICI), 2017, pp. 564-569.

[7] M. A. AlShargabi, A. Shaikh, A. S. Ismail, Enhancing the quality of service for real time traffic over optical burst switching (obs) networks with ensuring the fairness for other traffics, PLOS ONE 10 (2016) 3 - 29.

[8] A. F. et al., Kiss: Stochastic packet inspection classi_er for udp traffic, IEEE/ACM Transactions on Networking 18 (5) (2010) 1505-1515.

[9] P. B. et al., Abacus: Accurate behavioral classification of p2ptv traffic, Computer Networks 55 (6) (2011) 1394 - 1411.

[10] P. Wang, X. Chen, F. Ye, Z. Sun, “A survey of techniques for mobile service encrypted traffic classification using deep learning”, IEEE Access 7 (2019) 54024-54033.

[11] P. B. et al., Abacus: Accurate behavioral classification of p2ptv traffic, Computer Networks 55 (6) (2011) 1394 - 1411.

[12] Z. SabahiKaviani, F. Ghassemi, Behavioral model identification and classification of multicomponent systems, Science of Comp. Prog. 177 (2019) 41 - 66.

[13] A. P. A. Dainotti, C. Sansone, Early classification of network traffic through multi classification, Traffic Monitoring and Analysis, Lecture Notes in Computer Science 6613 (2011) 122-135.

[14] T. Battestilli, H. Perros, A performance study of an optical burst switched network with dynamic simultaneous link possession, Computer Networks 50 (2) (2006) 219 - 236.

[15] H. e. a. Kim, Internet traffic classification demystified: Myths, caveats, and the best practices, in: Proc. of the 2008 ACM CoNEXT Conf., CoNEXT'08, ACM, 2008, pp. 11:1-11:12.

[16] C. Tseng, G. Huang, T. Liu, P2p traffic classification using clustering tech nology, in: 2016 IEEE/SICE Int. Symp. on Sys. Int.(SII), 2016, pp. 174-179.

[17] Y. Q. et al., Discriminators for use inflow based classification, in: IEEE INFOCOM 2009, 2009, pp. 648-656.

[18] A. Moore, D. Zuev, M. Crogan, Packet classification algorithms: From theory to practice, in: Department of Computer Science Research Reports, Queen Mary, Univeristy of London, 2013, pp. 1-16.

[19] X. Li, M. J. Freedman, Scaling ip multicast on datacenter topologies, in:In Proc. of the 9th ACM Conf. on Emerging Networking Experiments and Technologies, 2013, pp. 61-72.

[20] S. Sen, O. Spatscheck, D. Wang, Accurate, scalable innetwork identification of p2p traffic using application signatures, in: Proceedings of the 13th International Conference on World Wide Web, WWW '04, 2004, pp.512-521.

[21] A. W. Moore, K. Papagiannaki, Toward the accurate identification of network applications, in: PAM, 2005.

[22] H. A. et al., Software defined networking: challenges and research opportunities for future internet, Computer Networks 75 (2014) 453-471.

[23] T. Auld, A. W. Moore, S. F. Gull, Bayesian neural networks for internet traffic classification, IEEE Transactions on Neural Networks 18 (1) (2007) 223-239.

[24] R. S. et al., Traffic classification using probabilistic neural networks, in: 2010 6th Int. Conf. on Natural Computation, Vol. 4, 2010, pp. 1914-1919.

[25] Hu Ting, Wang Yong, Tao Xiaoling, Network traffic classification based on kernel selforganizing maps, in: 2010 International Conference on Intelligent Computing and Integrated Systems, 2010, pp. 310-314.

[26] G. DraperGil, A. H. Lashkari, M. S. I. Mamun, A. A. Ghorbani, Characterization of encrypted and vpn traffic using timerelated features, in: ICISSP, 2016.

[27] B. Y. et al., Application identi_cation via network traffic classification, in: 2017 Int. Conf. on Computing, Net. and Comm.(ICNC), 2017, pp. 843-848.

[28] C. Tang, L. Song, J. Balasubramani, S. Wu, S. Biaz, Q. Yang, H. Wang, Comparative investigation on csma/ca based opportunistic random access for internet of things, IEEE Internet of Things Journal 1 (2) (2014) 171-179.

[29] S. S. Chawathe, Analysis of burst header packets in optical burst switching networks, in: 2018 IEEE 17th Int. Sym. on Network Comp. and App. (NCA), 2018, pp. 1-5.

[30] T. Q. et al., Ergid: An efficient routing protocol for emergency response internet of things, Jour. of Net. and Comp. Applications 72 (2016) 104 - 112.

[31] J. Shen, H. Tan, J.Wang, J.Wang, S. Lee, A novel routing protocol providing good transmission reliability in underwater sensor networks, J. Internet Technol. 16 (1) (2017) 171-178.

[32] J. Huang, Q. Duan, Y. Zhao, Z. Zheng, W. Wang, Multicast routing for multimedia communications in the internet of things, IEEE Internet of Things Journal 4 (1) (2017) 215-224.

[33] L. Song, S. Wu, H. Wang, Simplex: Symbollevel information multiplex, IEEE Internet of Things Journal 3 (5) (2016) 757-766.

[34] F. Tang, B. Mao, Z. M. Fadlullah, N. Kato, On a novel deep learning based intelligent partially overlapping channel assignment in sdn iot, IEEE Comm. Magazine 56 (9) (2018) 80-86.

[35] (2019 (accessed on Dec 20, 2019)). [link].URL https://archive.ics.uci.edu/ml/datasets.php

[36] J. Friedman, Greedy function approximation: a gradient boosting machine, The annals of statistics 2 (2001) 1189-1232.

[37] J. Friedman, T. Hastie, R. Tibshirani, Additive logistic regression: a statistical view of boosting, The annals of statistics 28 (2) (2000) 337-407.

[38] L. Breiman, Bagging predictors, Mach. Learn. 24 (2) (1996) 123-140.