IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁙ Impact Factor 8.102 ⁙ Peer-reviewed / Refereed journal ⁙ Vol. 12, Issue 5, May 2023

DOI: 10.17148/IJARCCE.2023.125153

NETWORK BORDER PATROL

Dr A B Rajendra[1], Sunil B[2], Sinchana S[3], Ritesh Kumar[4], Harshitha B S[5]

Dept. of Information Science and Engineering, Vidyavardhaka College of Engineering, Mysore[1-5]

Abstract — In the virtual world, the presence of network perimeter protection is essential. With the exponential growth of the Internet, networks are facing more and more problems. In certain cases of traffic jams or congestion drops, packets could not be delivered because there was no longer enough bandwidth available on the router link. Because you receive more packets than your router can handle. And the router's buffer size is overflowed by the packet. The main purpose of this research is to design and implement a congestion avoidance technique called "Network Border Patrol".

This affects routers (ingress, egress, core stateless) that need to regulate traffic to avoid undelivered packets or packet loss to provide a better quality of service. Specific network simulators should be used to visualise exactly how some algorithms can prevent congested links from collapsing. The algorithms are simulated in NS3 to test their performance and optimize network performance, improving QoS, and identifying areas for improvement. The results obtained demonstrate the effectiveness of the algorithms in regulating network traffic, optimizing traffic flow, and improving packet drop and congestion collapse.

Keywords — Computer network, Congestion collapse, Leaky bucket, Token bucket, Rate control algorithm, ingress and egress routers.

I. INTRODUCTION

Packet loss, queueing delays, or the blocking of new connections are all symptoms of network congestion, which lowers the quality of service. When a network connection or node carries more data than it can process, network congestion frequently results. Congestion on the road is demonstrated here.

Network Border Patrol is a novel technology for managing Internet traffic. The fundamental idea behind Network Border Patrol (NBP) is to compare the speeds at which packets from each application flow enter and leave a network at its boundaries. The network is probably buffering or, worse still, rejecting the packets from the flow if they are entering the network quicker than they are leaving it. In other words, the network is experiencing packet overload. By "patrolling" the network's boundaries, NBP avoids this scenario by making sure that no flow packets enter the network faster than they can exit. This patrolling ensures that competing network flows are treated fairly and minimises congestion breakdown causedby undelivered packets.

The scalability argument conveys the fundamental tenets of the Internet. There should be no new protocol, algorithm, or service added to the Internet unless it can scale properly. The end-to-end topic is a significant result of the scalability issue. We must move as much computational complexity as we can to the network's edge in order to ensure scalability. The finest illustration of Internet philosophy might be found in TCP congestion control. In the final system, algorithms are implemented to a large extent to achieve this. Regrettably, TCP Congestion Control also reveals several flaws in the end- to-end case.

The current Internet has two issues as a result of the stringent end-to-end congestion management implementation. Undeliverable packet congestion and a disparity in bandwidth between competing traffic streams. The first issue is when bandwidth is continually used by packets that are lost before they reach their destination, and congestion of undelivered packets collapses. Unacknowledged streams, which are more common on the Internet as a result of the widespread usage of audio and video-based network applications, are a key factor in the collapse of this sort of congestion, although the Internet currently effectively controls them. lacks aptitude.

In packet-switched computer networks, congestion can preclude or restrict meaningful communication, a state known as congestion collapse, often referred to as network performance collapse. Congestion is frequently reduced when a network "bottleneck" appears. In this instance, the total inbound traffic on the node is greater than the available outgoing bandwidth. The point where the local area network and the wide area network are connected is most likely the bottleneck.

II. LITERATURE REVIEW

The physical characteristics of the environment where a wireless sensor network is hosted may be monitored. In packet-switched computer and telecommunications networks, the leaky bucket [1] is a method used to monitor the flow of data in the form of packets with regard to previously established bandwidth and burstiness limitations. In order to avoid network latency, this [2] research suggested improving the method with a useful proposed token bucket size. The Token Bucket algorithm's bucket size is the manipulated variable, and it has been changed such that the method works better when applying delays. In order to provide the efficient recommended token bucket size that can be employed in wired networks and evaluated using OPNET modeller, the variables of this approach are adjusted. This technique has been successful in reducing network traffic delays and enhancing response times when consumers request many apps at once.

The Dynamic Token Bucket method (DTBA), developed by Tatsuya Fukui and colleagues in 2022 [3], enhances the traditional token bucket method by using a dynamic token supply. Due to its dynamic control over the token supply, experiments on DBS implemented in hardware showed that DTBA may produce packets within the shaping delay. The capacity of DBS to shape bursts, independent of the duration and timing of input, was confirmed by measured outcomes. They have demonstrated that DBS can achieve deterministic networks capable of providing strong End-to-End delay determinism even if each flow has varied delay needs without affecting network accommodation efficiency through studies that analysed the input of numerous traffic flows.

Due to the fact that it does not arbitrarily discard packets when aql is between the min and max limits, this method [4] seeks to provide better congestion control. The simulation model is based on ns-2, and a buffer management strategy called Adaptive Gentle Adaptive Random Early Detection (AGARED) is used to generate a bottleneck between nodes r1 and r2. The simulation outcomes demonstrated the suggested method's viability since it resolves recognised issues with the most well- known congestion control algorithm, RED.

A unique approach has been put out by researchers [5] to enhance TCP-friendly rate control (TFRC) across wireless networks. A well-liked rate control method called TFRC was created for unicast multimedia flows that operate in Internet environments and compete with TCP traffic. It is governed by the TCP throughput equation, which provides TFRC three benefits in rate control: it can prevent network connection collapse due to congestion, it preserves fairness with TCP flows, and it is better suited for real-time streaming applications. The throughput equation of TCP regulates the rate at which TFRC sends packets, giving it three benefits over other rate control algorithms: it prevents network connection collapse due to congestion, upholds fairness with respect to TCP flows, and is better suited for real-time streaming applications. The research [6] proposes an efficient method for data packet transmission error identification and correction in wireless communication networks.

The main framework for congestion control on the Internet is the Transmission Control Protocol (TCP) [7] congestion avoidance algorithm. When a connection or node is carrying so much data that the quality of its service suffers, it indicates that network congestion has occurred. Researchers and colleagues suggest modifying the fundamental TCP congestion control algorithm to improve its performance on wireless networks. In order to prevent congestive collapse, congestion control involves regulating traffic input into a communications network. Researchers and colleagues suggest modifying the fundamental TCP congestion control algorithm to improve its performance on wireless networks.

In order to address the problem of Internet congestion, this research [8] provides a joint method that combines a cross-layered mechanism with a stochastic approach and Markov modelling. Networking with less complexity in its routing and communication processes is the only option allowed under the current Internet architecture principles. To reduce the likelihood of congestion in a widely dispersed system, the suggested system combines a cross-layered method, stochastic approach, and Markov modelling. Delay, latency, and channel capacity are examples of network quality metrics that are not thought to be effective for congestion control. This study suggests a reliable TCP congestion control method that performs well under a range of network situations, including packet loss and RTT.

The existing NBP rate-control algorithm is intended to manage the ingress rates of flows to minimise router buffer occupancies, maximise link utilisation, and minimise congestion collapse. It does this by employing a method like TCP, which checks the state of the network and modifies the ingress rates of flows as necessary. A set of per-flow transmission rates that guarantee all packets are transmitted without inducing congestion collapse are determined by the method. Additionally, it dynamically modifies the rates in response to changes in network parameters like connection bandwidth or free buffer space. This guarantees that the network maintains stability and dependability while operating at a high level of efficiency. The pace at which packets are transferred from a source is regulated by the leaky bucket algorithm, which shapes traffic. It works by keeping a fixed-capacity buffer or bucket in which packets are deposited as they come in. The feedback control algorithm in NBP relies on exchanging ICMP packets between edge routers to provide forward and backward feedback.

ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁙ Impact Factor 8.102 ⁙ Peer-reviewed / Refereed journal ⁙ Vol. 12, Issue 5, May 2023

DOI: 10.17148/IJARCCE.2023.125153

III. METHODOLOGY

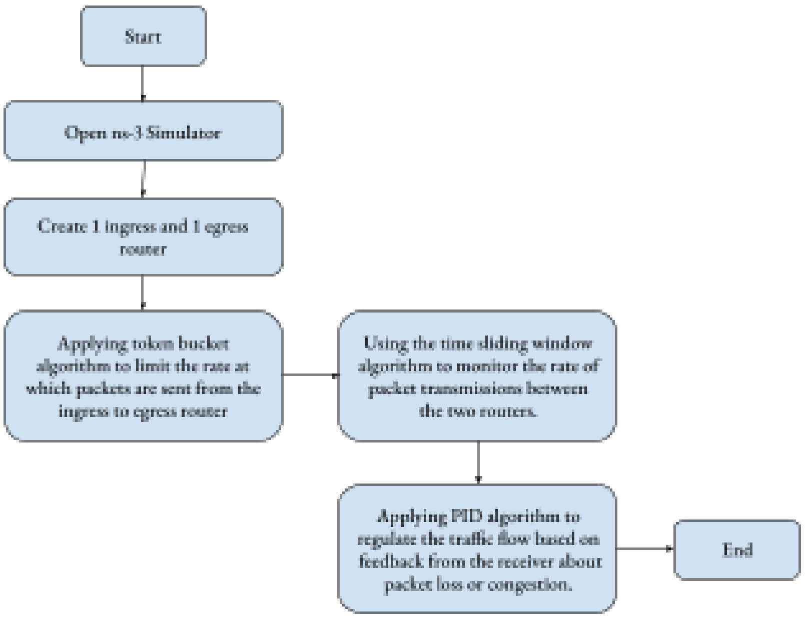
Start
Open ns-3 Simulator
Create 1 ingress and 1 egress router
Applying token bucket algorithm to limit the rate at which packets are sent from the ingress to egress router
Using the time sliding window algorithm to monitor the rate of packet transmissions between the two routers.
Applying PID algorithm to regulate the traffic flow based on feedback from the receiver about packet loss or congestion.
End

Figure 1. Proposed Flow Diagram

The Network Border Patrol is a stateless approach to avoiding congestion. In other words, it is consistent with the core stateless method, which for routers at the edges (or borders) of the network, but not for routers in the core, permits thread categorization and per-thread state preservation. Figure 2 displays this flowchart. We shall more clearly differentiate between two types of edge routers in this essay. Depending on the thread it operates on, an edge router can be thought of as either an incoming or an outgoing router. While outgoing routers handle network traffic leaving the network, incoming routers are edge routers that handle network flows entering the network.

A. Architecture

The edge router is the only network element that requires modification of the NBP. The input router's output ports and the output router's input ports must be modified to perform per-stream rate control and bitrate monitoring, respectively. In order to communicate and manage the entrance, it is also necessary to modify the ingress and egress routers.

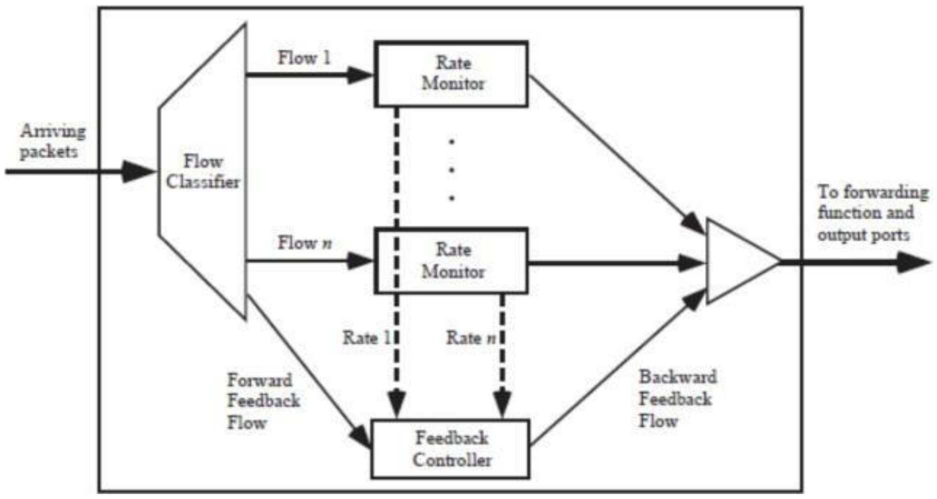

Fig 2. An input port of an NBP egress router

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 5, May 2023

DOI: 10.17148/IJARCCE.2023.125153

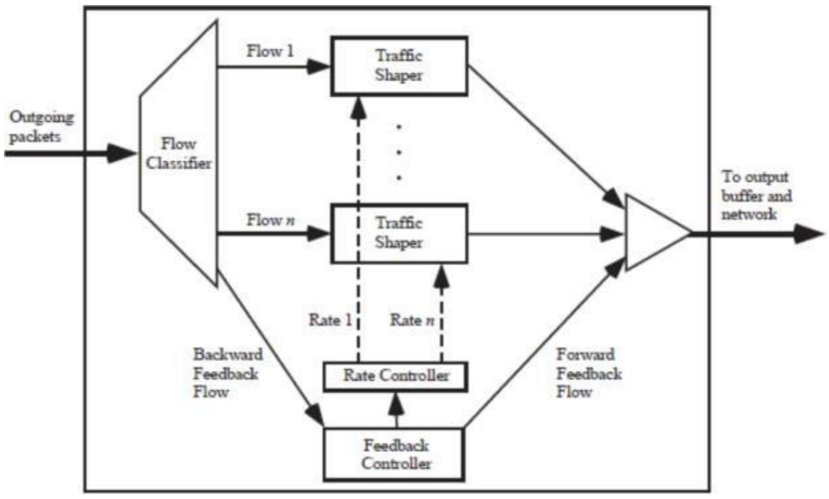

Fig 3: An input port of an NBP ingress router

An NBP egress router's gateway design is shown in Figure 2. The input router sends packets to the input port of the output router, where they are first sorted by the stream. For IPv6, this is accomplished by looking at the traffic label in the packet header, whereas for IPv4, this is accomplished by looking at the packet's source and destination addresses as well as the port number. Then, a bit rate estimate technique, such as Time Sliding Window (TSW), is used to track the bitrate of each stream. When a forward response packet from the route router arrives, the response controller collects these rates and delivers them back to the arriving router in feedback packets. head there.

The output ports of the NBP ingress routers have also been enhanced. Each one has a per-flow traffic shaper (like leaky buckets), rate controller, feedback controller, and flow classifier. While the flow classifier organises packets into flows, the traffic shapers control entry rates for packets from certain flows. The feedback controller receives backward feedback packets from egress routers and sends their contents to the rate controller. Additionally, it creates forward feedback packets, which it routinely transmits to the network's egress routers. The rate controller alters the parameters of the traffic shaper using a rate control method that is comparable to TCP.

B. Algorithms

Rate estimation algorithm in Egress Router -

Token Bucket: This algorithm uses a token bucket to control the flow of data packets. Tokens are added to the bucket at a fixed rate, and each packet sent out of the router requires a certain number of tokens. If the bucket is empty, the router will buffer packets until more tokens areadded.

Time sliding window in Egress Router -

In a Time Sliding Window (TSW) algorithm, the egress router uses a sliding window to keep track of the recent bandwidth usage over a certain period of time. The window is divided into fixed-size time intervals, and for each interval, the router records the number of packetssent and the amount of data sent. By looking at the window, the router can estimate the average bandwidth usage over the last few intervals, and use this information to control the flow of traffic. The TSW technique is straightforward to use and uses less memory, but it might not be able to recognise burst traffic or determine the precise amount of bandwidth that is available on high- speed networks. TSW is not a stand-alone rate estimate algorithm, it should be mentioned. Typically, it functions as a part of the active queue management (AQM) algorithm. A router's buffer condition is monitored by AQM algorithms, which also regulate the speed at which packets are sent out. The TSW algorithm is used to determine whether to discard packets in the event of congestion and to assess the most recent bandwidth consumption. So TSW, along with RED, BLUE, and PI, is a component of the AQM algorithm.

Flow Control Algorithm in Ingress Router -

Token Bucket: This algorithm uses a token bucket to control the flow of data packets. Tokens are added to the bucket at a fixed rate, and each packet sent into the network requires a certain number of tokens. If the bucket is empty, the router will buffer packets until more tokens are added.

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 5, May 2023

DOI: 10.17148/IJARCCE.2023.125153

Feedback control algorithm to calculate when to exchange feedback between Ingress and Egress routers

Proportional Integral Derivative (PID) algorithm - This algorithm uses feedback from the egress router to adjust the rate of packet transmission from the ingress router. In order to change the rate of packet transmission, the PID algorithm analyses the desired and actual rates of packet transmission. Three parameters—proportional, integral, and derivative—are used by the PID algorithm. Based on the present discrepancy between the desired and actual transmission rates, the proportional parameter is used to modify the rate of packet transmission. Based on the cumulative error over time, the Integral parameter is utilised to modify the rate of packet transmission. Based on the rate of change of the error, the Derivative parameter is used to modify the rate of packet transmission.

C. Time Sliding Window

In a Time Sliding Window (TSW) algorithm, the egress router uses a sliding window to keep track of the recent bandwidth usage over a certain period of time. The window is divided into fixed-size time intervals, and for each interval, the router records the number of packets sent and the amount of data sent. By looking at the window, the router can estimate the average bandwidth usage over the last few intervals, and use this information to control the flow of traffic.

The basic idea of the TSW algorithm is to estimate the bandwidth available to the egress router by measuring the number of packets and bytes transmitted during a certain time window. A time window is defined as a number of time intervals of a fixed duration. At the beginning of each time interval, the router measures the number of packets and bytes transmitted during the previous interval. The router can then use this information to estimate the average bandwidth usage over the last few intervals.

The sliding window algorithm can be used to estimate the available bandwidth in a number of ways, such as:

- By averaging the number of packets sent over the last few intervals: This gives an estimate of the maximum possible bandwidth available to the router.
- By averaging the amount of data sent over the last few intervals: This gives an estimate of the average bandwidth usage over the last few intervals.
- By comparing the number of packets or bytes sent in the last interval to the average over the last few intervals: This can be used to detectchanges in the traffic pattern.

The TSW algorithm is simple to implement and requires less memory, but it may not be able to detect burst traffic, or accurately estimate the available bandwidth in high- speed networks.

Time Sliding Window (TSW) is a type of algorithm that can be used for rate estimation. It works by measuring the number of packets or bytes transmitted during a certain time window and using this information to estimate the average bandwidth usage over the last few intervals. By looking at the window, the router can estimate the average bandwidth usage over the last few intervals, and use this information to control the flow of traffic. The TSW algorithm is simple to implement and requires less memory, but it may not be able to detect burst traffic or accurately estimate the available bandwidth in high-speed networks.

It should be noted that TSW is not a standalone rate estimation algorithm. It's usually used as a component of an active queue management (AQM) algorithm. AQM algorithms are designed to monitor the buffer status of a router and control the rate at which packets are sent out. The TSW algorithm is used to measure the recent bandwidth usage and make decisions on when to drop packets in case of congestion. So TSW is a part of the AQM algorithm like RED, BLUE, and PI.

D. Feedback Control Algorithm

Feedback control algorithms are used to calculate when to exchange feedback between ingress and egress routers, in order to optimize network performance. One example of a feedback control algorithm is the Proportional Integral Derivative (PID) algorithm. This algorithm uses feedback from the egress router to adjust the rate of packet transmission from the ingress router. The PID algorithm compares the desired rate of packet transmission to the actual rate and then uses this information to adjust the rate of packet transmission.

DOI: 10.17148/IJARCCE.2023.125153

Three parameters—proportional, integral, and derivative—are used by the PID algorithm. Based on the present discrepancy between the desired and actual transmission rates, the proportional parameter is used to modify the rate of packet transmission. Based on the cumulative error over time, the Integral parameter is utilised to modify the rate of packet transmission. Based on the rate of change of the error, the Derivative parameter is used to modify the rate of packet transmission. Another example of a feedback control algorithm is the Congestion Control Algorithm (CCA), which uses feedback from the egress router to adjust the rate of packet transmission from the ingress router. CCA monitors the buffer occupancy and queuing delay at the egress router and adjusts the rate of packet transmission from the ingress router accordingly.

These are examples of feedback control algorithms that can be used to calculate when to exchange feedback between ingress and egress routers. The choice of algorithm will depend on the specific requirements of the network and the goals of the feedback control system.

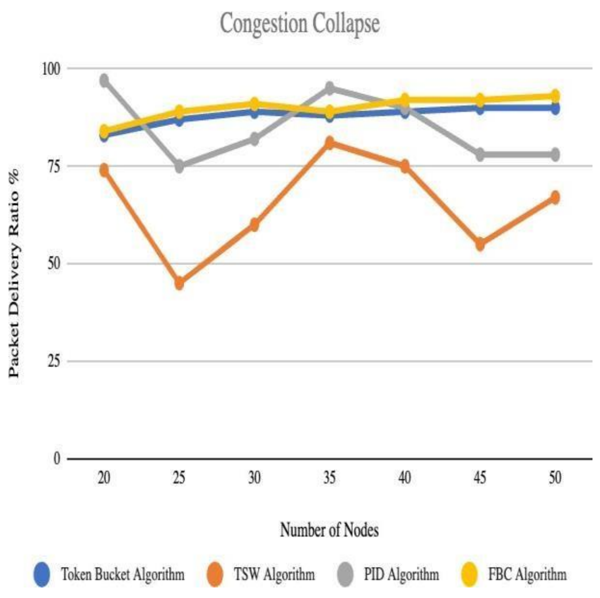

Figure 5. Congestion Collapse vs Number of Nodes

IV. SIMULATION

NS3, a popular network simulator that enables the construction of complicated network topologies, traffic patterns, and QoS requirements, is utilised for the simulation. Various network characteristics, including network traffic, packet loss, latency, and throughput, are evaluated throughout the simulation to assess how well the algorithms perform in various scenarios. The simulation's results may be utilised to enhance network performance, packet loss ratio, congestion collapse, and pinpoint problem regions

Table 1. Default Simulation Parameters

Time	120 s
Node Speed	20 m/s

The Simulation Defaults are predefined values used in the NS3 Network Simulator that provide a starting point for simulation tests. These values are often chosen to represent typical network conditions and are based on experimental data, industry standards, or previous research. Some of the default emulation settings in NS3 include network topology, traffic patterns, packet size, latency, and bandwidth. The network topology is usually modelled as a graph, with nodes

DOI: 10.17148/IJARCCE.2023.125153

representing network devices and edges representing network links. Traffic patterns can be defined as combinations of different types of traffic such as TCP, UDP, and CBR. The packet size is usually set to a default value, such as 1500 bytes, which is the maximum transmission unit (MTU) size for most networks. The delay and bandwidth values are also set to default values, which can be adjusted according to the specific requirements of the simulation experiment.

Simulation Parameter	Value
Number of nodes	30

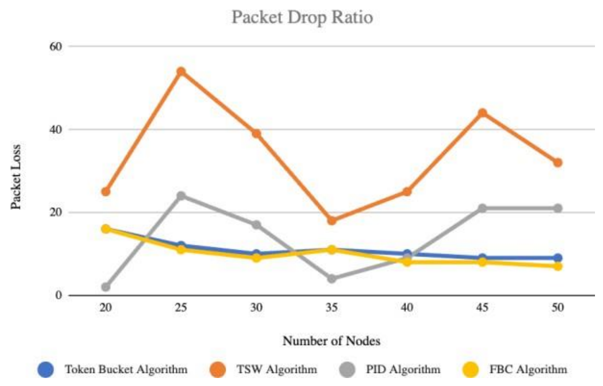

Figure 4. Packet Drop Ratio vs Number of Nodes

V. CONCLUSION

The Token Bucket Algorithm, Time Sliding Window, and Feedback Control Algorithm are efficient tools for controlling the flow of traffic between ingress and egress routers, guaranteeing a predetermined quality of service (QoS), and controlling the rate of outgoing and incoming traffic. A trustworthy platform for evaluating and improving network performance, packet drop, congestion collapse and pinpointing problem areas is provided by the simulation of these methods in NS3.

Future work may include integrating machine learning algorithms, simulating more complex network topologies and traffic patterns, implementing real-time monitoring and analysis tools to provide insights into network performance, and implementing additional traffic-shaping techniques. These developments can increase the network's effectiveness, scalability, and durability while ensuring appropriate QoS for a range of network applications.

REFERENCES

[1] Jiage Huo, K. L. Keung, C. K. M. Lee, Kam K. H. Ng,K.C. Li, "The Prediction of Flight Delay: Big Data-driven Machine Learning Approach," 2020 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM), Dec 2020.

Yushan Jiang, Yongxin Liu, Dahai Liu, Houbing Song, "Applying Machine Learning to Aviation Big Data for Flight Delay Prediction," 2020 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress(DASC/PiCom/CBDCom/CyberSciTech), Aug 2020.

[2] Bo Zhang, Dandan Ma, "Flight Delay Prediction at An Airport using Machine Learning," 2020 IEEE Xplore, Oct 2020.

[3] Fan Liu, Jinlong Sun, Miao Liu, Jie Yang, Guan Gui, "Generalized Flight Delay Prediction Method Using Gradient Boosting Decision Tree," 2020 IEEE 91stVehicular Technology Conference (VTC2020-Spring),May 2020.

[4] Guan Gui, Fan Liu, Jinlong Sun, Jie Yang, Ziqi Zhou, Dongxu Zhao, "Flight Delay Prediction Based on Aviation Big Data and Machine Learning," IEEE Transactions on Vehicular Technology, Nov 2019.

[5] Weinan Wu, Kaiquan Cai, Yongjie Yan and Yue Li, "An Improved SVM Model for Flight Delay Prediction," Conference on Digital Avionics Systems (DASC), April 2019.

[6] Bo Zhang, Dandan Ma, "Machine Learning Model- based Prediction of Flight Delay," International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Nov 2020.

[7] Xiaotong Dou, "Flight Arrival Delay Prediction And Analysis Using Ensemble Learning," IEEE Information Technology, Networking, Electronic and AutomationControl Conference, May 2020.