Shodhshauryam, International Scientific Refereed Research Journal
© 2019 SHISRRJ | Volume 2 | Issue 2 | ISSN : 2581- 6306

Internetwork Congestion-Avoidance and Collapse-Prevention Framework in Mobile Data Using Network Border Patrol Protocol

Akaninyene U. Ntuen[1], John E. Efiong*[2]
[1]Department of Computer Science, The Federal Polytechnic, Afikpo, Ebonyi State, Nigeria
*[2]Department of Computer Science, Wesley University, Ondo, Ondo State, Nigeria

ABSTRACT

The effectiveness of the Internet depends on the ability of network administrators and mobile network service providers to implement measures that are capable of preventing congestion problems in the Internet. Studies have shown that the current Internet suffers congestion problem as a result of many users contending for connections, resources and communication needs. This becomes more critical with the current proliferation of mobile and handheld devices. It therefore, becomes imperative to develop a congestion-avoidance mechanism to address this problem. This paper investigates and proposes a Mobile device-based Network Border Patrol (mNBP) protocol as a suitable rule for circumventing the problem identified in the information superhighway in mobile devices. The aim is to reveal the possible causes of congestion in mobile device-based internetworks and proffer a solution capable of leading to free flow of information in the internet. The implementation of mNBP framework will ensure free flow of packets as transmitted, successful arrival of packets to and from the Internet and avoidance of delay, drop or loss of packets in the Internet.

Keywords : Network Border Patrol (NBP), Internet, Mobile Device, Congestion collapse, Network Congestion-avoidance, Edge Router, Core Router, End System.

I. INTRODUCTION

In the current dispensation of computing avalanche, it is certain that every individual or organization depends on the use of computers, especially mobile devices driven by internet for several purposes, including information exchanges and resource-sharing. This has been proven to be cost-effective, time-saving, energy-preserving and hazard-free. Mobile devices are small, portable devices, capable of performing smart functions. They range from smartphones, personal digital assistants, iphones, notebooks, etc [1]. These devices depend heavily on internet availability for optimal utilization of their networked features [2]. As information is simply a processed and meaningful presentation of data, timely delivery of information enhances the productivity and optimal performance of an organization. Every organization, irrespective of size, business line or location, now depends on information for important decision making [3] . This way, information becomes an asset to businesses. Thus, in a bid to finding an effective and efficient means of information exchanges and resource sharing with mobile devices, the Internet prides itself in business. This Internet is a global system of interconnected computer networks that uses the Transmission Control Protocol (TCP) and Internet Protocol (IP) to facilitate data transmission and exchange [4].

Due to the rising need for timely, current and accurate information in the global marketplace orchestrated by the vast penetration of mobile devices, the Internet has now experienced an explosive growth over the past few years and with that growth has come severe congestion problems. To address this problem, this paper investigated and proposes a novel congestion-avoidance mechanism called Mobile device-based Network Border Patrol (mNBP) for implementation on mobile device-based networks which seeks to prevent the occurrence of congestion in the internet as a result of many users contending for connections and resources while communicating with their handheld computing devices.

Previous studies have assessed the internet congestion problem and identified probable remedies for preventing the maladies. There has been focus on improving the quality of service, enhancing packets flow rate, bandwidth management techniques, improving users' experience on the Internet of Things, etc. basically for computer-based users. Dedicated concentration has not been made on the present dispensation of smart devices – mobile devices which consume internet more than most other computer devices.

The several resources that run on each smart device are capable of using as much bandwidth as what about five computers would. This is so due to obvious reasons – the mobile devices are portable, meaning the users move about with them and spend more time on them than desktop networked computers and finally, the applications in them constantly perform automatic updates and synchronization. More problems are encountered with the current internet infrastructure with mobile devices where there is loss of packets on transit, waste of resources arising from packets being dropped or delay enroute the destination. This paper considers the possible implementation of NBP for mobile-based networks.

The rest of the paper is structured as follows: the second section presents the review related works to the study. Here, conceptual clarification is done. Factors and indicators of network congestion with effects on mobile users are explored. In section three, the proposed method is presented and discussion made in section four. Section five concludes the paper, followed by references.

II. RELATED WORKS

Literature has shown tremendous efforts made by researchers to proffer solutions to the current internet congestion problem. Some of the models proposed and designed in the past have been specific in addressing the congestion collapse problems while others have been general in proposing congestion control solutions [5]. Sasipraba and Srivatsa proposed a novel congestion avoidance mechanism for improving Quality of Service (QOS) in wireless networks using Network Border Patrol (NBP) [6]. In their study, they identified some general techniques for controlling and managing bandwidth to allow unrestricted flows of packets to and from where needed.

The study modeled NBP as a suitable approach for end-to-end congestion control, capable of resolving the current Internet problems by preventing congestion collapse from undelivered packets. The focus of the paper was on enhancing the QOS of the Internet Service Providers for computer-based slow internet experience using rate control, leaky bucket, time sliding window and rate monitoring algorithms. Authors in [7] modeled and analyzed a congestion control technique in the Internet of Things (IoT) using an improved Random Early Discard (IRED) algorithm. The paper performed simulations to evaluate performance of the model and used a queuing theory for the analysis of the performance. By comparing it with regular RED algorithm, the study showed that the proposed IRED has comparable delay performance and better

throughput performance than the standard RED, making IRED more suitable for IoT [8]. Besides defining some important concepts, this section explores indicators and factors of mobile internetwork congestion with their effects on mobile users.

A. Conceptual Clarifications

In the context of this study, congestion control defines an attempt to prevent an occurrence of a situation where the packets sent over a network from a source get dropped or lost by a router because of its inability to handle packets beyond its capacity, having its queue filled with packets already. Packets can be transported from different sources on the network to the router at the same time and may demand delivery to same or different destinations. This, in most cases may result to congestion situation which requires immediate notification and control [9]. Congestion collapse is a resource-wasting phenomenon on the network. According to [10]-12], a congestion collapse is said to occur where all the resources carried along with a packet from the source computer are wasted along the way as a result of one or more packets not being delivered. As a packet get dropped on transit due to congestion problem, the resources that would have aided the transportation of other packets to the destination are thrown away and wasted in the network.

This resource-loss is a subject of concern for network providers and has provoked studies in recent times. In this wise, network border patrol (NBP) is being investigated as a suitable algorithm for circumventing the menace. NBP is an Internet traffic control protocol that controls the transmission of packets at the borders of a network by patrolling the network's borders and exchanging feedback between routers at the borders of a network, thereby ensuring that each flow's packets do not enter the network at a rate greater than they are able to leave the network. Network Border Patrol (NBP) is to ensure that the transmitting channels or paths are not congested; packets are not delay or lost in the course of transfer. Thus, the implementation of Network Border Patrol (NBP) at the edge routers will guarantee successful packet delivery and mutual access to network shared resource.

B. Indicators and Factors of Mobile Internetwork Congestion

There are common indicators of congestion in the Internet which basically include increased network delay and dissatisfaction to users. On the delay axis, since all computer networks have a limited data carrying capacity, when the load is light, the average time for the exchange of information is relatively short but when many users are contending for connections and are actually communicating, the average delay increases. This delay has the effect of making the network appear "slower", because it takes longer time to send the same amount of data under congested conditions than it does when the load is light [13]. In extreme circumstances, an application can fail completely under a heavy network load and Session may timeout and disconnect [14]. With respect to dissatisfaction to users, Internet speeds are partly subjective which implies that the ultimate measure of Internet congestion is whether or not users can get their work done efficiently. And if users do not derive sufficient benefits from the internet services, it simply means a failure on the Internet performance.

However, it is also true that user dissatisfaction with performance may not indicate congestion in the Internet. The delay may be due to several factors such as the type of applications running, CPU speeds, hard disk performance, server and WAN access devices (including slow modems or WAN connection).

Several factors are responsible for congestion problems on the internet. This may be hardware related or software-based. For instance, there is a problem of link congestion. This occurs when the amount of traffic destined for a particular link exceeds the capacity of that link. When this happens, the switch or router buffers some packets, but eventually packets are discarded. Sensitive user's applications realize that a packet was lost, slow down their transfer speed, and re-transmit the data. If this was a file download, an email, or another non real-time application, the effect will be minimal as long as the packet loss does not continue to happen. Sadly though, some applications are not sensitive enough to handle this quite well such that the effect becomes noticeable to the users [15]. Congestion is most common at the entrance to a wide area network where the high capacity LAN meets a lower capacity access link, and at the exit from the wide area network where the service provider's large network meets the lower capacity access link. Traffic report plays an important role here. The essence of a traffic report is to show that a network's links are not over-utilized, and that the hardware utilization is within specification.

Faulty hardware or cabling is another cause of congestion malady. Here, malfunctioned physical components of the network is a bane to internet usage and can cause leakage or transmission of misleading data. If the hardware is not working properly, it will usually lead to error messages being seen on the console of the device or within system logs. If there is a link issue, it can usually be seen as errors on an interface. This can be seen on both copper cabling and fiber optic. It has been observed that even when the bandwidth is adequate, mobile device users can still face connection difficulties or congestion challenge the router, switch or firewall is not able to keep up with the traffic. The poor performances of these devices are worrisome. In addition, software issues, involving bugs on a network device can also pose a challenge and contribute to transmission problem. The presence of bugs in a network can cause network infrastructure to collapse or make old new features to fail [19].

C. Effects of Mobile Internetwork Congestion

In the existing system, packets are buffered in the routers present in the network. Data buffer (or just buffer) is a region of a physical memory storage used to temporarily store data while it is being moved from one place to another [16]. If they are packets waiting to be transferred before data arrives, then it must wait its turn before being sent across the transmission link (this is known as queuing). If the router has reached its full capacity, it won't have room for the new data to wait (queue), so it does the only thing it can, which is to discard the information. When congestion occurs in the Internet, it results to packets delay, dropped packets, packet loss, and out of order delivery. When congestion occurs in the Internet it might take a long time for packet to reach its destination because it gets held up in long queues, or takes a more indirect route to avoid congestion.

Again, the router might fail to deliver (drop) some packets, if the packet arrives when the router buffers are already full [14]. Packets could arrive the router when it is full due to congestion. All of the packets might be dropped, or none of them, depending on the state of the network and there is no way to tell which is advance. The receiving application must ask for this information to be retransmitted, and this will often cause a severe hiccup in transmission. Packet loss can occur for a variety of reason including link failure, high level of Internet congestion that lead to buffer overflow in router, Random Early Detection (RED), Ethernet problems, and the occasional misrouted packet. In communication, packet loss causes degradation in voice quality if packet loss concealment (PLC) is used then isolated losses may be less noticeable [1].

Packets loss requires recovery at the transport layer of the OSI model which consumes enough time to have a very noticeable effect on the application level response time experienced by an individual user. Retransmitted packets also have a tendency to exacerbate the congestion problem since retransmissions add to the traffic load in the Internet.

III. METHODS AND MATERIAL

The paper uses the unified modeling language in edraw to specify the model design. The architecture presented in figure 1 shows two network domains with end systems, edge and core routers. The core routers reside within the bodies of network, called the domains while the edge routers are positioned at the borders of the network to keep watch of packet flow or data patrol. Hence, the name network border patrol.

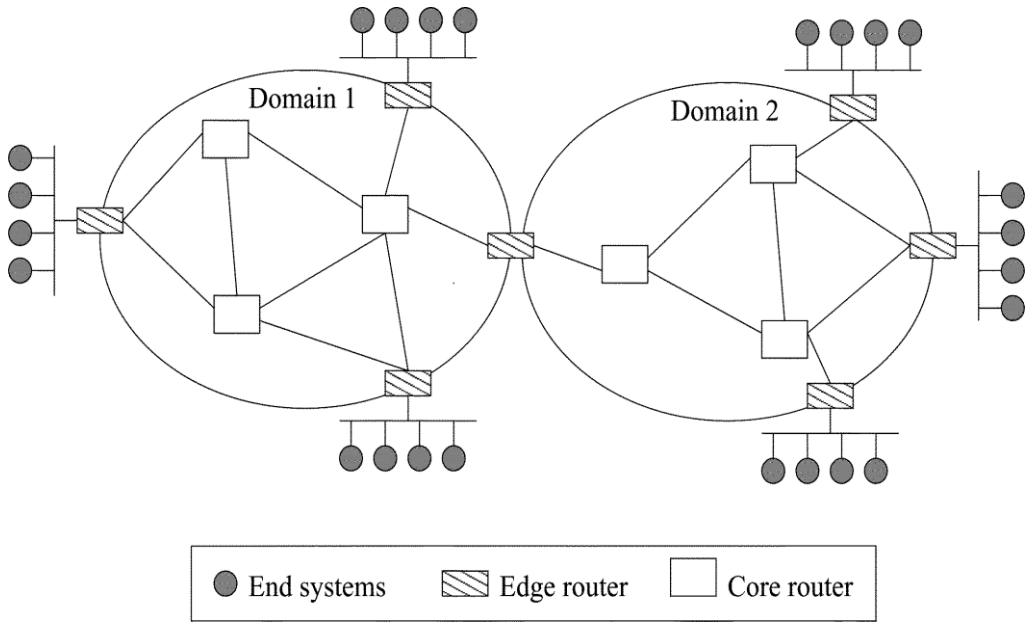

Fig 1. The Architecture of mNBP [17]

For the implementation of the mNBP, three routing classifiers are used – basically an end system, edge router and core router. An end system is a device that is connected directly to the Internet, creating an interface that individual mobile device users can access. End systems take numerous forms. They allow users to interact directly with the Internet to send and receive data and they may be used for everything from processing orders for a company to sending out photographs of a family vacation. One example of an end system is a smart phone or cellular phone. The phone has applications that people can use to perform tasks like checking email, browsing the Internet, uploading files, and so forth. In addition to phones, devices such as cameras, personal digital assistants can also be connected to the Internet as end systems, as seen when people use webcams to chat with each other.

An edge router is simply a router that connects the network one controls to a network that one does not have control over. In most cases, it is the router that is connected directly to the user's internet connection. It transfers data between a local area network and a wide area network, choosing the most effective paths to use when sending or receiving data. It gets its name from the fact that it

sits at the periphery, border, or edge, of a network. A core router on the other hand is a router that forwards packets to hosts within a network (but not between networks). It is a router designed to operate in the Internet backbone, or core. This is pictorially presented in figure 2, showing the data flow of the mNBP.

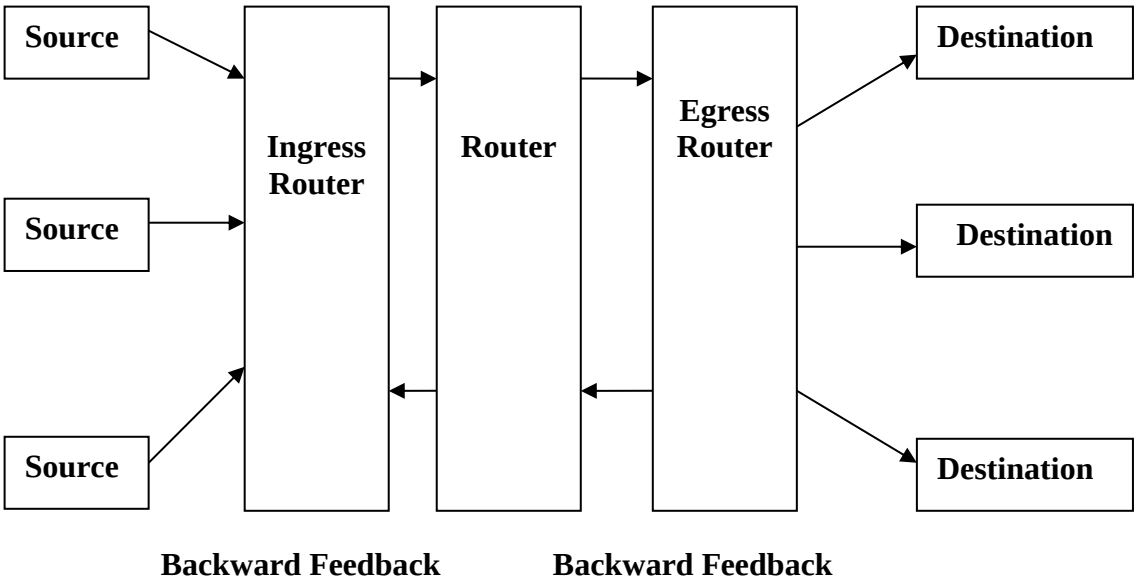

Fig. 2. Data Flow Diagram of the mNBP [18]

IV. RESULTS AND DISCUSSION

The mNBP entails the exchange of feedback between routers at the borders of a network in order to detect and restrict traffic flows before they enter the network, thereby preventing congestion in the Internet. The basic principle of the mNBP is to compare, at the borders of a mobile network, the rates at which packets from each mobile application flow are entering and leaving the network. If a flow's packets are entering the network faster than they are leaving it, then the network is likely buffering or, worse yet, discarding the flow's packets. In other words, the network is receiving more packets than it is capable of handling. The mNBP prevents this scenario by "patrolling" the network's borders, ensuring that each flow's packets do not enter the network at a rate greater than they are able to leave the network. This patrolling prevents congestion in the internet.

Although mNBP is capable of preventing congestion collapse in the Internet, this improvement does not come for free. NBP solves these problems at the expense of some additional network complexity, since routers at the border of the network are expected to monitor and control the rates of individual flows in mNBP. The mNBP also introduces added communication overhead, since in order for an edge router to know the rate at which its packets are leaving the network, it must exchange feedback with other edge routers. However, mNBP's added complexity is isolated to edge routers; routers within the core of the network do not participate in the prevention of congestion collapse. Moreover, end systems operate in total ignorance of the fact that mNBP is implemented in the network, so no changes to transport protocols are necessary at end systems. Depending on which flow it is operating on, an edge router may be viewed as ingress or egress router. An edge router operating on a flow passing into a network is called an ingress router, whereas an edge router operating

on a flow passing out of a network is called an egress router. Note that a flow may pass through more than one egress (or ingress) router if the end-to-end path crosses multiple networks.

The mNBP prevents congestion through a combination of per-flow rate monitoring at egress routers and per-flow rate control at ingress routers. Rate monitoring allows an egress router in figure 3 to determine how rapidly each flow's packets are leaving the network, whereas rate control allows an ingress router to police the rate at which each flow's packets enter the network. Linking these two functions together are the feedback packets exchanged between ingress and egress routers; ingress routers send egress routers forward feedback packets to inform them about the flows that are being rate controlled, and egress routers send ingress routers backward feedback packets to inform them about the rates at which each flow's packets are leaving the network as shown in figure 4. By matching the ingress rate and egress rate of each flow, NBP prevents congestion within the network.

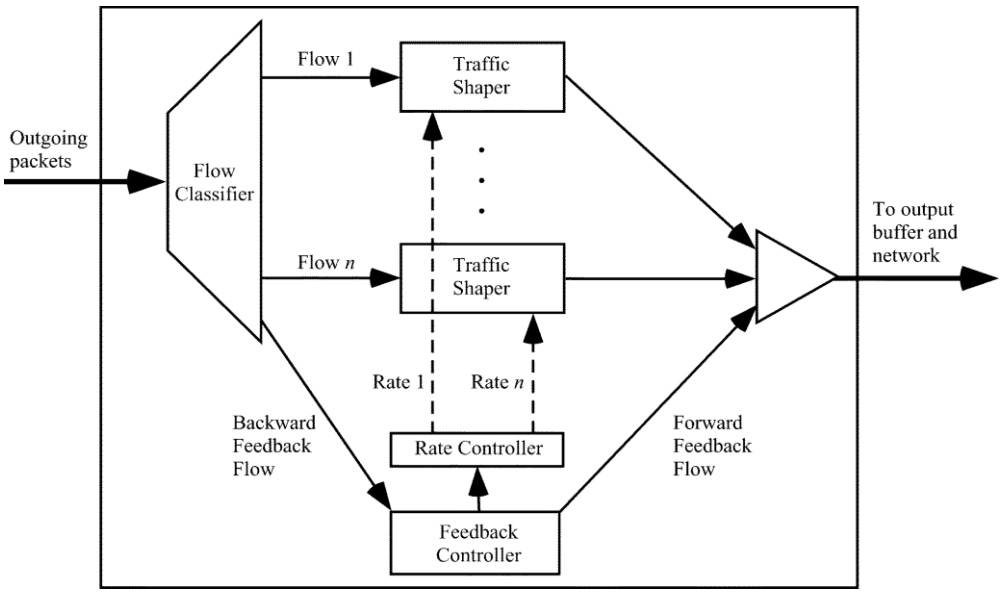

Fig. 3 : Input Port of an mNBP Egress Router [17]

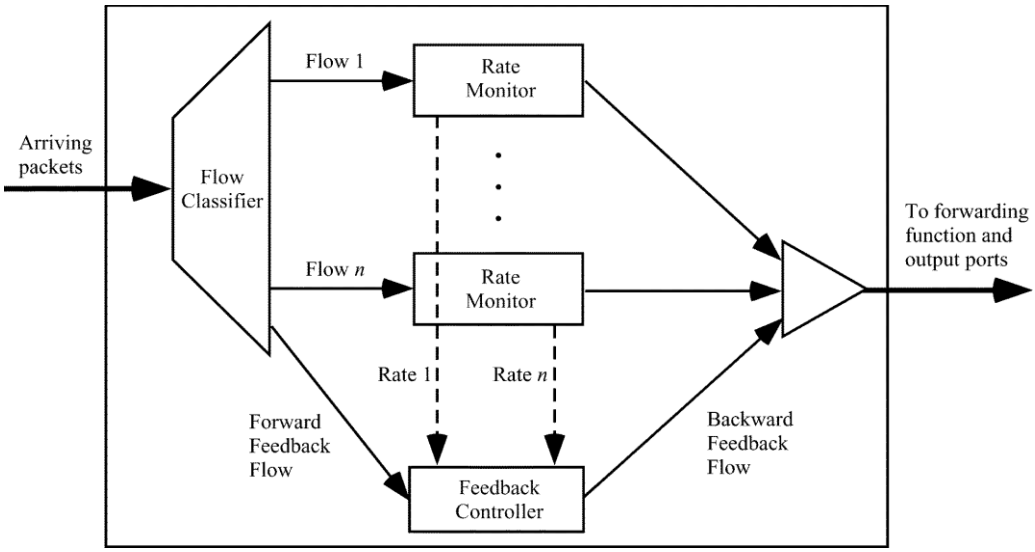

Fig. 4 : Output Port of an mNBP Ingress Router [17]-[18]

V. CONCLUSION

In today's fast paced mobile technology world, the usage of the Internet increases, and the data sending over the mobile network increases such as multimedia files which occupies much space leads to congestion in the Internet. This paper emphasizes on designing and implementing of a mobile device-based congestion-avoidance mechanism called mobile Network Border Patrol (mNBP) that will monitor and control congestion in the Internet or traffic problems that do occur in the current system. The mNBP allows buffering of packets to be carried out in the edge routers rather than in the core routers. The packets are then sent into the network based on the capacity of the network and hence there is no possibility of any undelivered packets present in the network. Absence of undelivered packets avoids overload due to retransmission.

The aim of the mNBP protocol is to ensure that the transmitting channels or paths are not congested; packets are not delay or lost in the course of transfer. Thus, the proposed model system is aimed at successful packet delivery and mutual access to network shared resource.

VI. REFERENCES

[1] L. Atzori, A. Iera, & G. Morabito (2010), "The internet of things: A survey," Computer Networks, 54(15), 2787 – 2805, Oct. 2010.

[2] K. K. Ramakrishnan & R. Jain (1990) "A Binary Feedback Scheme for Congestion Avoidance in Computer Networks with a Connectionless Network Layer," ACM Transactions on Computing Systems, 8(2), 158–181, May 1990.

[3] S. Zhuravlev, s. Blagodurov & A. Fedorova, (2010) "Addressing Shared Resource Contention in Multicore Processors via Scheduling". In ACM SIGARCH Computer Architecture News, Vol. 38, No. 1, 129-142, March 2010.

[4] W. Lehr, j. Peha & S. Wilkie, (eds) (2007), Special Section on Network Neutrality: International Journal of Communication (volume 1, 2007), August 2007.

[5] S. Keshav, (2007) "What is congestion and what is congestion control", Presentation at IRTF ICCRG Workshop, PFLDnet 2007, Los Angeles (California), USA, February 2007.

[6] T. Sasipraba, S. K. & Srivatsa (2013), "Network Border Patrol, a Novel Congestion Avoidance Mechanism for Improving QOS in Wireless Networks. Information Technology Journal, 5: 427-432. **DOI:** 10.3923/itj.2006.427.432.

[7] J. Huang, D. Donggai, Q. Duan, Y. Sun, Y. Yin, T. Zhou, & Y. Zhang, (2014) "Modeling and Analysis on Congestion Control in the Internet of Things". IEEE ICC 2014 - Ad-hoc and Sensor Networking Symposium,. 434-439, 2014.

[8] J. Wu, Hassan, M., & Jha, S., (2001)," QPD: A packet discard mechanism for multimedia traffic in the internet", IEICE Transactions and. Communications., 538-541, 2001.

[9] K. Ramakrishnan, Floyd, S., & Black, D. (2001) "The Addition of Explicit Congestion Notification (ECN) to IP', RFC 3168, September 2001.

[10] V. Jacobson, (2001) "Congestion Avoidance and Control". ACM Computing and. Commununications, 1: 45-52, 2001.

[11] J. Nagle, "Congestion Control in IP/TCP Internet Works Internet". Engineering Task Force, 2: 78-86, 2002.

[12] F. J. Vazquez-Abad & Krishnamurthy, V. (2002), "Self Learning Call Admission Control for Multimedia Wireless DS_CDMA systems". Proceeding of the 6th

International Workshop on Discrete Event Systems, 2002, Zaragoza, Spain, 399-404.

[13] Firoiu, V. and M. Borden, (2000),"A Study of Active Queue Management for Congestion Control", Proceedings of IEEE INFOCOM'00, Tel Aviv, Israel, March 2000.

[14] C., Albuquerque, Vickers, B. & Suda, T. "Network Border Patrol". IEEE Transactions and Communications, 1: 158-167, 2000.

[15] N. Dukkipati and McKeown, N., (2006.), "Why Flow-Completion Time is the Right Metric for Congestion Control", ACM SIGCOMM Computer Communication Review, Vol. 36, No. 1, January 2006.

[16] S. Floyd, & Fall, K., (2011), "Promoting the use of End-To-End Congestion control in the Internet". IEEE/ACM Transactions Network., 2: 234-243, 1999.

[17] S. Murugesan, Gangadharan, G., & John, R., (2012), "Avoiding Congestion Control Using Network Border Patrol", International Journal of Computer Science and Information Technologies, 3(5) , 2012, 5243-5246.

[18] J. Singh, J., and M. A. Lambay, (2016), "Network Border Patrol: Preventing Congestion Collapse and Promoting Fairness in the Network", ISAR International Journal of P2P Network and Techniques, 1(1), Jan – Feb 2016, www.internationaljournalisar.org.

[19] P. Chhabra, Chuig, S., Goel, A., John, A., Kumar, A., Saran, H., & R. Shorey, (2002) "XCHOKe: Malicious Source Control for Congestion Avoidance at Internet Gateways," Proceedings of IEEE International Conference on Network Protocols (ICNP'02), Paris, France, November 2002.

Cite this article as :