A Novel Approach for Efficient Bandwidth Utilization in Transport Layer Protocols

Sakshi Garg, Purushottam Sharma and Varsha Singh

Abstract The Internet has in a flash developed into an incomprehensible worldwide system in the developing innovation. TCP/IP Protocol Suite is the fundamental necessity for nowadays Internet. Web use keeps on expanding exponentially. The TCP/IP suite has many plan shortcomings so far as transfer speed, bandwidth utilization, and congestion are concerned. Some of these are protocol outline shortcomings, though rest is deformities in the product that executes the protocols. The real accentuation is on protocol-level issues, as opposed to execution defects. The paper discusses about the packet transmission issues identified with the connection-less and connection-oriented protocols in the transport layer. Subsequently, an approach is proposed for the overcoming of the weaknesses and expanding transmission capacity and decreasing congestion in the network and succeeds in giving the proposed solution complexity as O(n) which is best, that can be practically achieved.

Keywords Internet · TCP/IP protocol · Security · Congestion
Bandwidth utilization · Transmission capacity · Packet retransmission
Connection less · Connection-oriented

S. Garg (✉) · P. Sharma · V. Singh
Amity School of Engineering and Technology, Amity University,
Noida, Uttar Pradesh, India
e-mail: sakshijyotigarg@gmail.com

P. Sharma
e-mail: psharma5@amity.edu

V. Singh
e-mail: varsha.singh502@gmail.com

V. Bhateja et al. (eds.), *Proceedings of the Second International Conference on Computational Intelligence and Informatics*, Advances in Intelligent Systems and Computing 712, https://doi.org/10.1007/978-981-10-8228-3_43

1 Introduction

The Internet Protocol suite [1] is the theoretical model and set of interchanges protocols utilized on the Internet and comparative PC systems. It is generally known as TCP/IP on the grounds that the first protocols in the suite are the Transmission Control Protocol (TCP) [2, 3] and the Internet Protocol (IP). It is sometimes known as the Department of Defense (DoD) model, in light of the fact that the improvement of the systems administration model was supported by DARPA, an organization of the United States Department of Defense [4]. The transport layer [5] in the TCP/IP suite [6] is situated between the application layer and the network layer. It gives administrations to the application layer and gets administrations from the network layer. It gives a procedure-to-process correspondence between two application layers, one at the nearby host and the other at the remote host [7, 8].

Transport layer has different protocols like Sliding Window Scheme [9], Stop-and-Wait Protocol, Go-Back-N, Selective Repeat and ARQ Technique for the above Protocols. These protocols lay controls for the exchange of bundle from sender to beneficiary. Each is a change of the other, however, no protocol clarifies the situation of retransmissions of the packets. Though there exists procedures like timeout based transactions, ARQ Technique and others but each of them deals with the accentuation on the transmission of packets not the retransmission of the similar packet. Such packets either get dropped or they are retransmitted over and over which increment clog at the network and furthermore squander the transmission capacity on the off chance that the parcel needs to hold up until Time to Live. Thus, in the paper a novel way to deal with this hitch in the network is proposed [10].

The principle commitment of this paper is to propose a contemporary approach for the transmission of packets from the sender to the back-to-back recipient which will aid in proficient bandwidth utilization and falling congestion [11, 12] in the system brought about due to the loss of packets and retransmissions. The paper is organized as follows. Section 2 holds the literature review. Section 3 exhibits a relative investigation of different transport layer protocols considering in space of both, connection-less and connection-oriented protocols took after by their working. Section 4 expresses the research gap, proposed solution to it and its preferences. In Sect. 6, results are outfitted for the same. Section 7 contains the conclusions on the exhaustive investigation of the transport layer protocols, the issues distinguished, proposed arrangement, and derivation from it. Ultimately, Sect. 8 furnishes the future scope and bearings.

2 Literature Review

Espina et al., in his paper described the development and the essential usefulness of the TCP\IP protocol. They attempted to uncover the reasons why the main data networks expected to advance to wind up what we know these days as the internet. At long last, a future view is point by point of what the current reviews and tried advances convey as the best answer for bolster the developing requests of the clients and technological upgrades [1]. Jacobson, Van, et al., revised the transport protocol and set forward RTP, the continuous transport protocol that gave end-to-end network transport capacities reasonable for applications transmitting ongoing data, for example, sound, video or recreation data, over multicast or unicast network administrations. The change he proposed was to the scalable timer algorithm for computing when to send RTCP packets keeping in mind the end goal to limit transmission in abundance of the planned rate, when numerous members join a session at the same time in the prior RFC 1889 [2].

Karnati Hemanth et al., gave the TCP/IP suite which has many outline shortcomings as far as security and protection are concerned. In his paper, he concentrated primarily on protocol-level issues, instead of execution defects. In his paper, he examined the security issues identified with the portion of the protocols in the TCP/IP suite [3]. Iren et al., reviewed Transport layer protocols accommodate end-to-end correspondence between at least two hosts. This paper introduced an instructional exercise on transport layer ideas and phrasing, and an overview of transport layer administrations and protocols. The administration and protocol elements of twelve of the most imperative protocols were condensed in his paper [5].

Randall et al., analyzed that a few applications as of now require more noteworthy usefulness than what either TCP or UDP brings to the table, and future applications may require considerably more. Like TCP, STCP offers an indicate point, connection-oriented, dependable conveyance transport benefit for applications imparted over an IP network. Perceiving that different applications could utilize a portion of the new protocol's capacities for call control motioning in voice-over (VoIP) networks, the IETF now holds onto SCTP as a broadly useful transport-layer protocol, joining TCP and UDP over the IP layer [6]. S. M. Bellovin, evaluated the TCP/IP protocol suite, which is broadly utilized today, was produced under the sponsorship of the Department of Defense. In spite of that, there are various genuine security flaws intrinsic in the protocols, regardless of the rightness of any executions. He depicted an assortment of attacks in light of these flaws, including sequence number spoofing, routing attacks, source address spoofing, and verification attacks and furthermore introduced protections against these attacks, and closed with a talk of wide range resistances, for example, encryption [7].

Balwinder Kaur et al., explained the data can get lost, reordered, or copied because of the nearness of switches and support space over the inconsistent divert in the traditional networks. The sliding window protocol will recognize and rectify

blunder if they got data have enough repetitive bits or rehash a retransmission of data. The paper demonstrated the working of this duplex protocol of data link network [9]. Prabhaker Mateti, explained the TCP/IP suite has many outline shortcomings so far as security and protection are concerned. Some of those are protocol plan shortcomings, while the rest are imperfections in the product that executes the protocols. In his paper, he depicted these issues from a useful point of view [10].

Purvang Dalal et al., conferred that the Transmission Control Protocol (TCP), an imperative transport layer correspondence protocol, is ordinarily tuned to perform well in customary wired networks, where Bit Error Rate (BER) is low and congestion is the essential driver of packet misfortune. He portrayed the issue by the conduct of wireless links and the parts of TCP operation that influence execution lastly, his report investigated a sorted examination of various existing arrangements similarly, as it is hard to make a "one size fits all" TCP for wireless networks [13]. M. Anand Kumar et al., examined that the network and Internet applications are developing quickly in the current past and the current security system was not satisfactory for today's applications. Since there is no protection for the application layer of the network model. He proposed security engineering for the TCP/IP Protocol Suite talked over Internet use keeps on expanding exponentially. So network security turns into a developing issue. Also, he introduced another design for TCP/IP protocol suite which ensures security to application layer utilizing a protocol Application Layer Security Protocol (ALSP) [14].

3 Various Transport Protocols

The TCP/IP protocol utilizes a transport layer protocol [15] that is either an adjustment or a mix of some of these protocols.

3.1 Sliding Window

Since the arrangement numbers utilize modulo 2m, a circle can speak to the grouping numbers from 0 to 2m − 1. The buffer is taken as an arrangement of slices, called the sliding window that involves some portion of the circle at any instance. At the sender site, when a packet is sent, the comparing slice is stamped. At the point when the slices are marked, it implies that the buffer is full and no further messages can be acknowledged from the application layer. At the point when an acknowledgment arrives, the comparing slice is unmarked. In the event that some successive slices from the earliest starting point of the window are unmarked, the window slides over the scope of the comparing arrangement numbers to permit all the more free slices toward the finish of the window. The succession numbers are in modulo 16 (m = 4) and the measure of the window is 7.

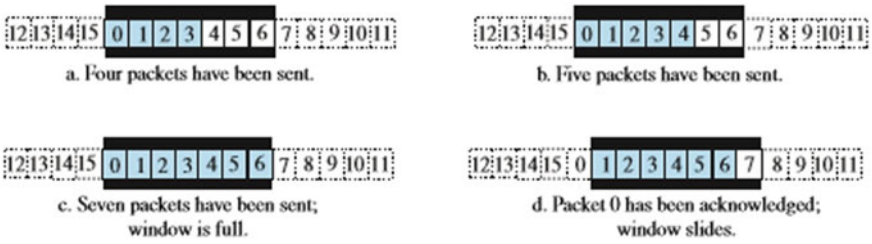

Fig. 1 Sliding window in linear format (*Source* [4])

Take note of that the sliding window is only a reflection: the genuine circumstance utilizes PC factors to hold the grouping quantities of the following packet to be sent and the last packet sent [4, 9] (Fig. 1).

3.2 Simple Protocol

Our first protocol is a basic connection-less protocol with neither stream nor mistake control. We accept that the recipient can quickly deal with any packet it gets. As it were, the collector can never be overpowered with approaching packets. Figure 4 demonstrates the format for this protocol (Fig. 2).

The transport layer at the sender gets a message from its application layer, makes a packet out of it, and sends the packet. The transport layer at the collector gets a packet from its network layer, removes the message from the packet, and conveys the message to its application layer. The transport layers of the sender and collector give transmission administrations to their application layers [2, 4].

3.3 Stop-and-Wait Protocol

Our second protocol is a connection-oriented protocol [11, 12] called the Stop-and-Wait protocol, which utilizes both stream and mistake control. Both the sender and the recipient utilize a sliding window of size 1. The sender sends one packet at any given moment and sits tight for an acknowledgment before sending

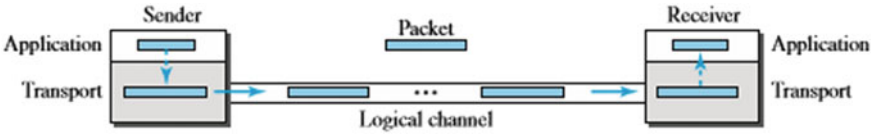

Fig. 2 Simple protocol (*Source* [4])

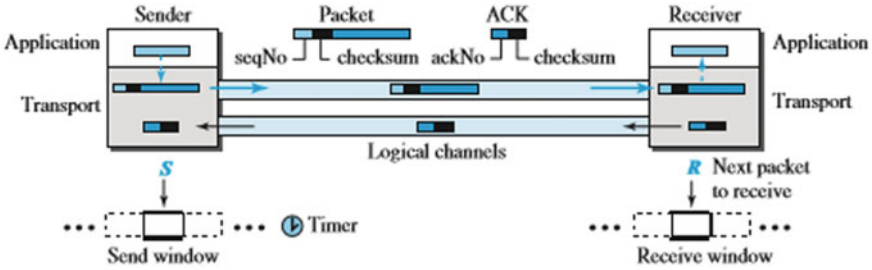

Fig. 3 Stop and wait protocol (*Source* [4])

the following one. To distinguish undermined packets, we have to add a checksum to every data packet. At the point when a packet reaches the collector site, it is checked. In the event that its checksum is off base, the packet is debased and noiselessly disposed of. The hush of the recipient is a flag for the sender that a packet was either ruined or lost. Each time the sender sends a packet, it begins a clock, if an acknowledgment arrives before the clock terminates, the clock is halted and the sender sends the following packet (on the off chance that it has one to send). On the off chance that the clock terminates, the sender resends the past packet, expecting that the packet was either lost or adulterated. This implies the sender needs to keep a duplicate of the packet until its acknowledgment arrives [4] (Fig. 3).

3.4 Go-Back-N Protocol (GBN)

To enhance the effectiveness of transmission [6, 14, 15] (to fill the pipe), numerous packets must be experiencing significant change while the sender is sitting tight for affirmation. As it were, we have to give more than one packet a chance to be extraordinary to keep the channel occupied while the sender is sitting tight for acknowledgment. In this segment, we examine one protocol that can accomplish this objective; in the following segment, we talk about a moment. The first is gotten back to Go N (GBN) (the sound of the name will turn out to be clear later). The way to Go-back-N is that we can send a few packets before accepting affirmations, yet the beneficiary can just buffer one packet. We keep a duplicate of the sent packets until the acknowledgments arrive, however, few data packets and acknowledgments can be in the channel in the meantime (Fig. 4).

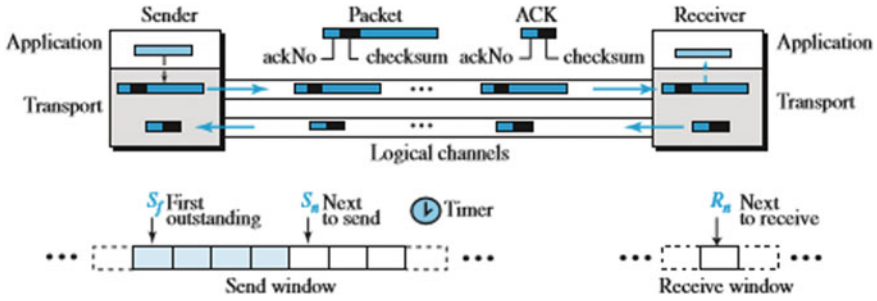

Fig. 4 Go-Back-N protocol (GBN) (*Source* [4])

3.5 Selective Repeat

The Go-Back-N protocol improves the procedure at the recipient. The beneficiary monitors just a single variable, and there is no compelling reason to buffer out-of-request packets; they are essentially disposed of. Be that as it may, this protocol is wasteful if the hidden network protocol loses a ton of packets. Each time a solitary packet is lost or adulterated, the sender resends every single extraordinary packet, despite the fact that some of these packets may have been gotten sheltered and sound however out of request. On the off chance that the network layer is losing numerous packets in view of congestion in the network, the resending of these extraordinary packets aggravates the congestion, and in the end, more packets are lost. This has a torrential slide impact that may bring about the collapse of the network. Another protocol, called the Selective Repeat (SR) protocol, has been concocted, which, as the name infers, resends just particular packets, those that are really lost [4] (Fig. 5).

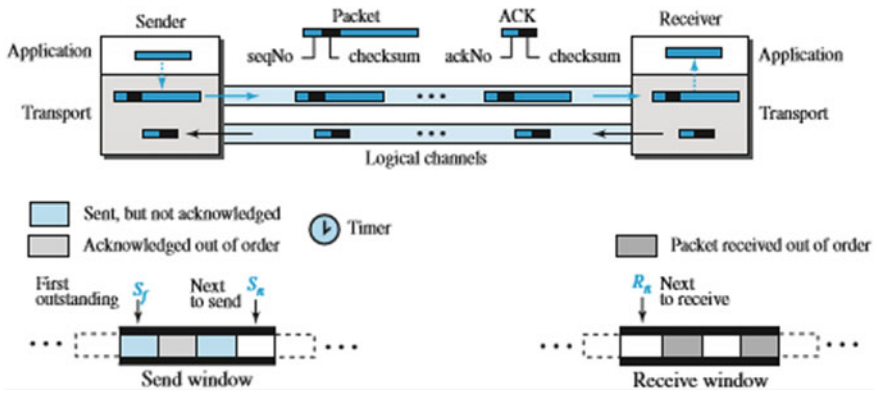

Fig. 5 Selective Repeat protocol (*Source* [4])

3.6 Automatic Repeat Request

Automatic Repeat reQuest (ARQ), otherwise called Automatic Repeat Query, is a mistake control strategy for data transmission that utilizes acknowledgements (messages sent by the beneficiary demonstrating that it has effectively gotten a data casing or packet) and timeouts (indicated time frames permitted to slip by before an acknowledgement is received) to accomplish solid data transmission over untrustworthy service. ARQ protocols can be classified into Stop-and-wait ARQ, Go-Back-N ARQ, and Selective Repeat ARQ/Selective Reject [7, 10].

4 Proposed Solution

The problem statement and solution to the problem identified can be given as follows.

4.1 Research Gap

(a) Factors after various literature surveys and findings it is seen that there is an anomaly in the transport layer protocols that although the protocols are efficient enough to send the packet from source to destination and each protocol has the revised features of the previous ones but none of the protocols takes into account the time being wasted to retransmit the packet that could not be sent due to network congestion, or loss of response, loss of acknowledgement, etc.
(b) It is necessary to know the time spent (rather the no. of the times the packet is retransmitted) to send the same packet again and again since it is wasting the bandwidth and creating congestion over the network by transmitting the same packet over and over again. Consequently, there exists no such framework that suggests any such policy.

4.2 Proposed Solution

Many researchers have progressed with plentiful techniques and algorithms to examine the security issues and other transmission related schemes. The emphasis here is on scrutinizing the gap analyzed during the literature reviews in the networking domain, which can be further explored for efficient retransmission of packets and effective utilization of bandwidth (Fig. 6).

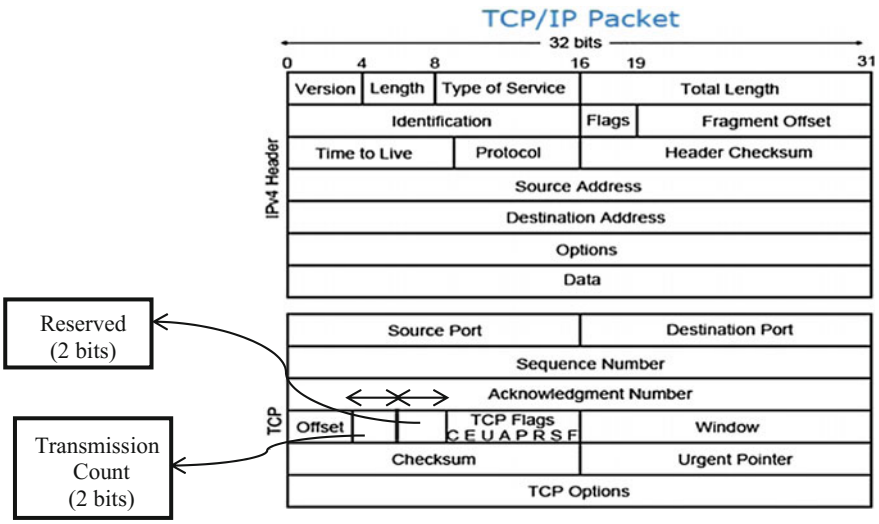

Fig. 6 Modified TCP/IP packet

5 Algorithm

Transmission Count

```
if (int m==0)
{
 trans_count=0;
}
else
{
while (m<15)
{
trans_count++;
}
delay();
}
```

Clock Delay

```
void delay(unsigned int result)
{
clock_t goal = result + clock();
while (goal > clock());
}
```

Random_Number Generator

```
int random_number (int min_num, int max_num)
{
int result = 0, low_num = 0,   high_num= 0;
if (min_num < max_num)
{
low_num = min_num; high_num = max_num + 1;
}
 else
 {
 low_num = max_num + 1;
 high_num = min_num;
 }
 srand (time(NULL));
  result = (rand() % (high_num - low_num)) + low_num;
 return result;
 }
```

//*Min to max range can be taken between (0 to 10)*//

5.1 Complexity of the Algorithm: O(n)

Since there can be n-number of such packets that have to be retransmitted over the network and each packet takes O(1) time complexity where m is the concerned packet to be retransmitted so, the overall complexity comes out to be O(n). This is the least time complexity one can achieve for this function for n-number of the packets to be retransmitted.

5.2 Justification of the Study

The solution proposed is such that it is taking 2 bits from the RESERVED field of the TCP/IP frame format and introducing an additional field of 2-bits called as transmission count.
This transmission count will keep an entry of the no. of times the packet is retransmitted that is not received at destination due to network reasons like congestion, loss of response, loss of acknowledgment etc.
If the no. of transmissions for the retransmitted packet exceeds 4, the packet shall wait for some random time that can be given by some Probability (p).

This will greatly reduce the traffic at the network by decreasing the no. of retransmission packets at the network and therefore, help in reducing network congestion.
Since definite and less attempts have to be made at a time to send the retransmission packet; this will be a great aid in reducing the wastage of the bandwidth.

6 Results and Discussions

6.1 Increased Bandwidth Utilization

Each time a packet is transmitted from source to goal, in existing cases the packet gets dropped if there should be an occurrence of network congestion and keeps up no mean numerous transmissions of a similar packet in the event that it cannot be conveyed at the primary example, thus data transfer capacity is squandered in it.

Utilizing the proposed calculation, since number of retransmission for the rehashed packets named as transmission count are fixed, so once that count is over then the packet will be transmitted simply after a random time with probability p. In this manner, in the network that packet will be sent simply after the irregular time with likelihood p which will diminish activity at the network, thus more data transfer capacity will be accessible for more packets to be transmitted. Consequently, it will give increased bandwidth utilization.

6.2 Less Network Congestion

In the network that packet will be sent simply after the arbitrary time with likelihood p after it has striven for one total round of Transmission Count, which will decrease activity at the network, thus will prompt less congestion in the network.

6.3 More Robust

Robust means the ability to withstand failures. Failures may occur due to network congestion which shall be recovered using the proposed model.

6.4 Reliable

When the packet cannot be sent at the first instance, it will be tried to send multiple times without keeping a count of number of retransmissions happens to send that packet and also in case of much network congestion the packet will be dropped which means some valuable information may be lost in the existing scenario. But the catch in the proposed approach is that since it is keeping a track of how many times the packet is retransmitted, assume that the packet is not transmitted in the first round of transmission count, then it will be transmitted after a random time with probability p which means the packet will not be dropped, it will be tried after that random time, that is no information will be lost, hence it will be more reliable.

6.5 Higher Efficiency

The overall complexity of the pseudocode comes out to be O(n) which is very less for n-number of packets to be the retransmitted as compared to the existing scenario. So, it has higher efficiency.

7 Conclusion

The current system takes after transmission of packets from source to goal where the packet gets dropped if there should arise an occurrence of network congestion and maintains no count for multiple transmissions of the same packet if it cannot be delivered at the first instance. While in the proposed approach, the packet will be sent simply after the arbitrary time with likelihood p which will decrease movement at the network, thus more transmission capacity will be accessible for more packets to be transmitted, less network congestion, more reliable, more robust, and higher effectiveness. Additionally, the general intricacy of the pseudocode is O(n), which is very less for n-number of packets to be retransmitted.

8 Future Scope and Directions

The future work of the proposed model is the simulation of the proposed algorithm using NS-2 tool.

References

1. Espina, David, and Dariusz Baha. "The present and the future of TCP/IP."
2. Jacobson, Van, et al. "RTP: A transport protocol for real-time applications." (2003).
3. Karnati Hemanth et al, "Security Problems and Their Defenses in TCP/IP Protocol Suite", International Journal of Scientific and Research Publications, Volume 2, Issue 12, December 2012, ISSN 2250-3153.
4. Forouzan, A. Behrouz. Data communications & networking (sie). Tata McGraw-Hill Education, 2006.
5. Iren, Sami, Paul D. Amer, and Phillip T. Conrad. "The transport layer: tutorial and survey." ACM Computing Surveys (CSUR) 31.4 (1999): 360–404.
6. Stewart, Randall, and Christopher Metz. "SCTP: new transport protocol for TCP/IP." IEEE Internet Computing 5.6 (2001): 64–69.
7. Bellovin, Steven M. "A look back at" security problems in the tcp/ip protocol suite." Computer Security Applications Conference, 2004. 20th Annual. IEEE, 2004.
8. Yongguang Zhang, Malibu, C.A. "A multilayer IP security protocol for TCP Performance enhancement in wireless networks", IEEE Journal on Selected areas in communication, 22(4), 767–776 (2004).
9. Kaur, Balwinder, et al. "Importance Of Sliding Window Protocoll." International Journal of Research In Engineering And Technology, EISSN: 2319-1163| PISSN: 2321-7308 (2013).
10. Mateti, Prabhaker. "Security issues in the TCP/IP suite." Security in Distributed and Networking Systems", World Scientific Pub Co Inc (2007): 3–30.
11. Sahu, Yaminee, and Sumit Sar. "Congestion Control Analysis in Network: A Literature Survey." (2016).
12. Chaudhary, Pooja, and Sachin Kumar, "A Review of Comparative Analysis of TCP Variants for Congestion Control in Network", International Journal of Computer Applications 160.8 (2017).
13. Dalal, Purvang, and K. S. Dasgupta. "TCP performance issues and related enhancement schemes over wireless network environment." International Journal 2.4 (2012).
14. Kumar, M. Anand, and S. Karthikeyan. "An Enhanced Security for TCP/IP Protocol Suite." Journal of Computer Science and Mobile Computing, Vol.2 Issue. 11, November-2013, pg. 331–338.
15. Abdelsalam, Ahmed, et al. "TCP Wave: A new reliable transport approach for future internet." Computer Networks 112 (2017): 122–143.