ISSN 2350-109X
www.indianscholar.co.in

Indian Scholar

An International Multidisciplinary Research e-Journal

SMART DATA PACKET MOVEMENT – ASSESSING A POSSIBLE WAY TO REDUCE NETWORK TRAFFIC

Atharv Garg
JBCN International School (Borivali)
mark.atharv@gmail.com

Abstract

The paper aims for a fail-proof model that expects to be given the modification rights in the Internet Layer or at a relay stations increasing speed and efficiency of the data packets that are being sent to and from sources and destinations.

Keywords:*Data Packets, Data Packets loss, Internet Protocol (IP) Routing methodology, Nodes, Client-Side Prediction, Packet switching, Carrier-sense multiple access with collision avoidance (CSMA/CA)*

INTRODUCTION

This paper outlines a way to predict traffic congestions. What effect does this bring to today's networking systems? (Focusing on the broad aspect: Internet) How often these congestions occur? Could these congestions be predicted using a neural network algorithm?

While reading this paper, one needs to have basic understanding of networking, data packet movements, Client-Side Prediction, CSMA protocols and various other access modes. Due to the increasing traffic on a large scale (World Wide Web A.K.A WWW), there are frequent "roadblocks" on the network.

To overcome these road-blocks various methods can be applied. Few of them consists of solving the roadblock by (i)sorting out which Data Packet gets priority to pass through, (ii)re-route the packet stuck in the roadblock, (iii)re-route the packet approaching the roadblock so that the block does not get out of control and/or (iv)close intakes on the particular network line.

The fourth (iv) case will rarely be used due to the fact that it becomes inefficient to close down a whole network line. Case three (iii) will be the case discussed in this paper. This action can also be performed by a forceful use of a switch but predictiveness of these roadblocks can help the network lines to work in more efficient way between a node-to-node communication.

Theory

To simulate a situation that is stated in Case three (iii). A closed network consisting of a mesh topology can be used. The topology consisting of six node points *(represented in the Fig. 1)*. The primary motive of the third (iii) case is to predict a problem and send out cautions to intermediate nodes so that they can re-route or route the data packets accordingly.

ISSN 2350-109X
www.indianscholar.co.in
Indian Scholar
An International Multidisciplinary Research e-Journal
MISA MEMBERS OF INTERNATIONAL SCHOOLS' ASSOCIATION

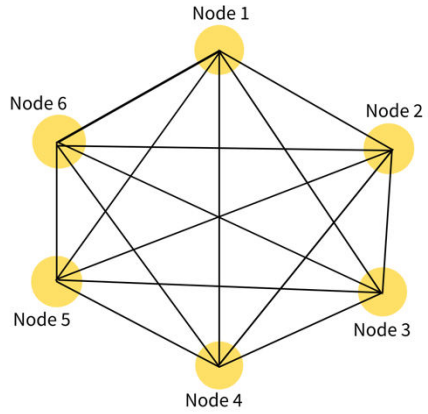

Fig. 1, A mesh topology containing six nodes

A data packet can travel from *Node 1* to *Node 4* without any obstructions in a straight path. Let's say suppose the particular network line is blocked due to traffic, the data packets can be re-routed to follow the path *Node 1*(origin) *to Node 2*(intermediate node) *to Node 3*(intermediate node) *to Node 4*(destination). This switch can also be performed using a switch or just sending out the data packets on that path but what if during the journey an overload of data packets occurs on a network line?

Addressing the motive of this paper, In the stated scenario a node will have the autonomy to re-route the chain of data packets if the allocated path has blockages. This autonomy can be gained by assessing previous traffic overloads on the network line, finding and using a simple neural network algorithm. A resonating technology called as Client-Side prediction has been a successful cheat in the world of game production.

Client-Side prediction creates an artificial image of the player, and its prime goal is to predict a player's movements and create a lag free environment for the receiving player. This is one way of addressing reduced network traffic but it has limitation of only being used in the field projection of already assessed data [1].

Continuing, The data packet travelling from *Node 1(origin) to Node 2(intermediate node)* encounters another network line blockage between *Node 3(intermediate node) to Node 4(destination)* to overcome this the data packets are routed to *Node 4* directly from *Node 2*.

In todays' autonomous world, this decision can either be made by predicting how often there are data packet loss between two nodes or by giving out an advisory to the preceding node received from the succeeding node. The latter case is quite impossible as a data packet is usually sent in the form of signals and there is not a way to give out caution advisory to the receiving node faster than a relay signal.

The reason for mentioning Client-Side prediction is What if the client could predict these roadblocks on certain relay lines? This could result to having the data packets consisting of another set of (optional) instruction containing information for the nodes that a particular network line has a chance of a blockage so send the data packet through another route.

Assessing a past made data packet loss prediction model, [2, Fig. 7] *In scenario 3(Fig. 2), the model got 65% data packet loss prediction accuracy for the farthest network (USA - Korea) tracking route for having loss of ≤20 packets was considered on the "no loss" side of the data collected.*

ISSN 2350-109X
www.indianscholar.co.in
Indian Scholar
An International Multidisciplinary Research e-Journal
MISA MEMBERS OF INTERNATIONAL SCHOOLS' ASSOCIATION

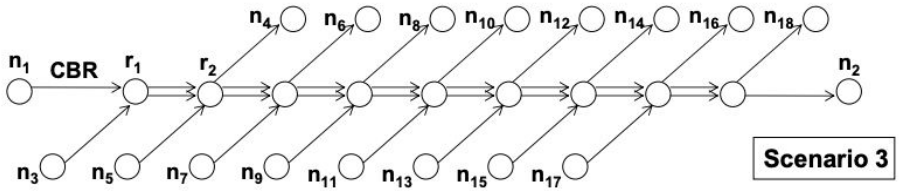

Fig. 2, scenario 3, extracted from [2, Fig. 7]

Since this model was tested in late 2005's, the accuracy of the model is subject to degrade due to better data lines and relay methods. Although, the same model with a bit of modifying can be used to predict the amount of packet loss on a particular data line. These figures could then be used to predict the time or conditions that are giving significant data packet loss.

Given that a Carrier-sense multiple access with collision avoidance (CSMA/CA) protocol sends out data frames to check whether the channel is clear or not, the node waits for a random period of time before checking again. This consumes a lot of time. CSMA/CD uses the data packets collided or lost on a data line to check if data line is clear or not, this sets of a random timer to send out the data packets again. This process is time and resource consuming.

A model which can predict on past collided data packetsand set a timer for a predicted time instead of a probability of 'p' time should be optimal for solving the issues with CSMA protocols. This gives the sovereignty to a node to decide and rectify the path of the data packet to a much more stable route without any significant data packet loss.

Recalling the statement about the possibility of adding another layer of instructions predicting the packet loss on a particular line can be included in the TCP/IP model. A complex calculation of creating a "Hoax" route, plotting out the points or time frames a data packet should encounter a blockage, optimal alternative routes, and the alternative routing instructions for the nodes.

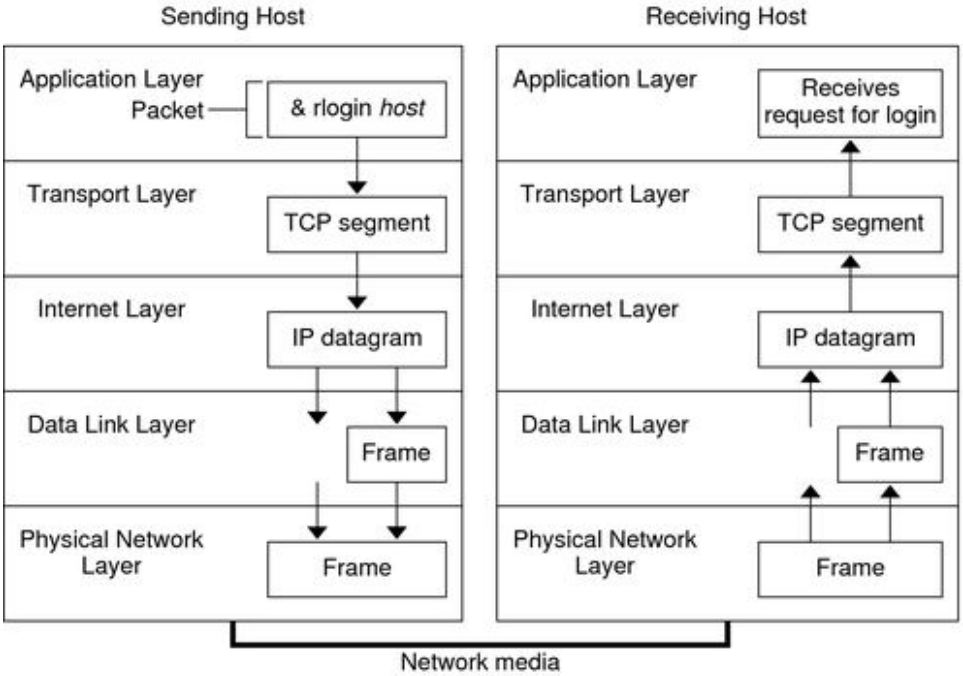

Fig. 3, TCP/IP Stack, extracted from [6, Fig. 1-1]

ISSN 2350-109X
www.indianscholar.co.in

Indian Scholar

An International Multidisciplinary Research e-Journal

MISA Global Partnership
MEMBERS OF INTERNATIONAL SCHOOLS' ASSOCIATION

In a TCP/IP connection, a proper and secure "three-way handshake" is required for the data packets to be forwarded to the receiving node. The Application layer sends out a login request to the receiving host and then further the Transport layer ensures that the data is reached in a reliable way. The Transport layer also creates a virtual path and attaches a header to each encapsulated data packet so that they are forwarded to the right track. If there are reports of data packets lost the protocol sends the data packets to the host again.

Since TCP is a connection-based protocol, it may not be suitable to real time data sending. UDP a "connectionless" protocol [6] does not check if all the packets have arrived at the destination or not. This makes it efficient but it reduces the quality of a real time image/video/game being projected to the user.

The Internet layer determines if the packet is in IP datagrams or not, this could be useful for the forwarding ports as if there is a need to edit the route the resonating datagrams could be edited efficiently.

A writeable functionality in the Transport Layer and the Internet Layer provided to the forwarding ports could determine a way of changing the routes. Even though protocols like PPP (Point-to-Point Protocol) have proved to be a secure connection with the internet, there are high expectations for it to have data packet loss.

The way a best routing is chosen is based on few factors depending on the dynamic protocols being used. [4] A hop count between source and destination (Routing Information Protocol, RIP), getting a cost based shortest route from source to destination (Open Shortest Path First, OSPF) and calculating the bandwidth, delay, load and reliability (Enhanced Interior Gateway Routing Protocol, EIGRP). A routing table helps the router to decide which route should be assigned to a data packet. Since these are considered to be the most efficient protocol and also use routing tables consisting pre-defined routes, there is a high possibility that they end up having multiple collisions due to them being overused.

Routing is the only stage where a data packet is given the complete freedom to be writable in terms of the route to be followed. Pre-defined routes do give a benefit of less processing power being used up for assigning routes. A paper discussing broadening the size of a routing table [5] has been presented in a previous conference. They have outlined a methodology using '*' to represent different addresses in Class A, B and C. The '*' is only to define the number that needs to be passed randomly.

The routing table model can be narrowed down by using multiple queries. A suggestion of implementing a 'delay' column could help the router decide what routes would be suitable. This delay accounts for the lines that are jammed; this delay could also be considered as the ping.

Considering the situation where the data packet has been assigned a route and is on its path, a line block while transportation is highly possible as well. As outlined before CSMA protocols could fail in high traffic cases. Giving a relay node to have read and writable function allows the incoming data packets to be re-routed.

The problem of how a node should decide whether to overwrite the current path arises. This requires the nodes to also have aninternet layer. Stated before, this layer could consist of a table that contains past data packet loss data and predicts whether a particular route is subject to have packet loss or a 'traffic jam' at a particular instance.

A relay node shall only have this forceful action after there has been a trigger. This trigger is set off if there are multiple data packets being lost in a short time, the data packets are not

ISSN 2350-109X
www.indianscholar.co.in
Indian Scholar
An International Multidisciplinary Research e-Journal
MISA MEMBERS OF INTERNATIONAL SCHOOLS' ASSOCIATION

completing the entire journey in the expected time, the CSMA/CD protocol fails on one particular network line and/or the data packets are not being sent at all for a prolong period of time.

n = number of packets being lost
k = number of packets not completing the journey in expected time t# (time in seconds)
p = number of data packets not being sent from a station after a period of time# (time in seconds)
j = number of times the protocol has failed
e = number of average failures, or the average time period in which the data packet is not considered to be stale

if n≥20:
refer to the routing table with predictive values and decide a new route
if k> 1:
refer to the routing table with predictive values and decide a new route
if p >e:
refer to the routing table with predictive values and decide a new route
if j > e:
refer to the routing table with predictive values and decide a new route

All of the above conditional statements having an else statement to repeat their original cycle and try again if it fails.

The system is aiming for a fail proof method that supports all other backups if one of the cases fails.

If the number of packets lost are more than or equal to 20 data packets (as stated by the data packet loss prediction model) the model moves onto a writeable state. The same state is achieved if the number of packets not reaching in the expected time of journey, if the number of packets not being sent after a period of time is not achieved (this value usually should be taking in account the maximum time the packet can be held at the station) and finally if the CSMA/CD protocol fails 'j' after a certain period of average failure 'e' decided by the past data.

This flexibility of relay nodes having the ability to write also requires them to acquire a routing table from their location to consider all the factors stated above.

If the writable state is not achievable by the succeeding nodes, then the previous nodes shall also consider adding in the optimal alternative routes in the routing header of a data packet.

ISSN 2350-109X
www.indianscholar.co.in

Indian Scholar

An International Multidisciplinary Research e-Journal

CONCLUSION

In totality, there are three significant ways there could a better model implemented. One, the nodes could be used to predict the blockage period using past data loss and route the incoming data packets to another network lines. Two, the data packets consisting of the TCP/IP model could have another layer of header consisting of the required information for the nodes to deviate from their path. Three, instead of having another layer, the relay nodes could rectify the current route to reach the destination in an optimal time predicted using a classification predictive model. This classification model takes in consideration of the values which are considered to be 'not the optimal time' and the values which are the 'optimal time'. Furthermore, an average from the optimal time could be taken to get the best results out of the data (assuming that it has no illegal values – many values that are not far away from being considered as either of the restrictions).

Acknowledgements

Mr. Shad Khatib (Computer Science teacher, JBCN International School (Borivali)), for guiding me through this theoretical research.

REFERENCES

[1] Y. W. Bernier, "Latency compensating methods in client/server in-game protocol design and optimization", presented at Game Developers Conference 2001, Mar 20, (Vol. 98033, No. 425).

[2] L. Roychoudhuri and E. S. Al-Shaer, "Real-time packet loss prediction based on end-to-end delay variation," in IEEE Transactions on Network and Service Management, Nov. 2005, vol. 2, no. 1 , pp. 29-38, doi: 10.1109/TNSM.2005.4798299.

[3] Tech Target Contributor, "CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance)", TechTarget Search Networking, https://searchnetworking.techtarget.com/definition/CSMA-CA (accessed June 28, 2021)

[4] Cisco press, "Cisco Networking Academy's Introduction to Routing Concepts", Cisco Press, https://www.ciscopress.com/articles/article.asp?p=2180208&seqNum=9 (accessed June 30, 2021)

[5] Draves, R.P., King, C., Venkatachary, S. and Zill, B.D., "Constructing optimal IP routing tables." In IEEE INFOCOM'99. Conference on Computer Communications. Proceedings. Eighteenth Annual Joint Conference of the IEEE Computer and Communications Societies. The Future is Now (Cat. No. 99CH36320) (Vol. 1, pp. 88-97). March, 1999.

[6] Oracle, "How the TCP/IP Protocols Handle Data Communications", OracleSystem Administration Guide: IP Services , https://docs.oracle.com/cd/E18752_01/html/816-4554/ipov-29.html (accessed July 17, 2021)