Journal of Theoretical and Applied Information Technology
31st October 2016. Vol.92. No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

UNDERSTANDING NETWORK CONGESTION EFFECTS ON PERFORMANCE - ARTICLES REVIEW

[1]MOHAMED NJ., [2]SHAHRIN SAHIB,[3]NANNA SURYANA, [4]BURAIRAH HUSSIN.
{[1, 2, &3]: ICT Faculty (FTMK), Universiti Teknikal Melaka Malaysia (UTeM)}
Emails: 1) mohamed1nj@gmail.com, 2) shahrinsahib@utem.edu.my, 3) nsuryana@utem.edu.my, 4)burairah@utem.edu.my]

ABSTRACT

Networking communications have become popular worldwide in human daily services. Network Congestion (NC) happens whenever because nodes and links are overloaded. Such situations affect the network expected performance and its services quality. Congestion /NC occurs as a results of its subnets' links overload, which gradually (overtime) affects the network performance with an increase of transmission delay, a slowdown of throughput as generally perceived by network's users. NC is considerable as the basis problem in network performance quality acceptance; and most of its existing problem solutions are expected still playing a great role in the future networks model, which will be running mostly too many multimedia applications. However, various researches over past years have initiated the study on the causes leading to congestion and, different lessons can be learnt from NC situations analysis to understand its relationship with the future network's performance. This paper presents an analytical review of NC occurrence causes and the fundamentals of the existing control solutions/frameworks as available and studied from some former and recent networks publications. A particular attention has been paid throughout this study to found out how NC may still affect the future networks performance (i.e. QoS in the world of multimedia networks). And the coverage/content of this paper is expected to serve as a quick access to the knowledge essentials for researchers on related subject as stated in this paper topic.

Keywords: *Communication, congestion, performance, service quality, QoS, network, networking, WLAN/LAN, choke point, congestion, edge router, flow, traffic, data rate, wireless.*

1. INTRODUCTION

Congested network refers to the moment in network's links when any new data entry to be sent to a destination will create instead a blocking effect into the transmission line. Thus, this may result primarily to throughput decrease with the data already admitted in process. According to [1],[2], the observed phenomenon signaling a congestion are data transmission delay, packet loss, and connections blocking. And all these happen as response/reaction of the links/nodes which are carrying more than expected data in transmission process. In other cases [4], NC refers to switched network moments when somewhere in lower levels, data (i.e. Packets #) put on the links exceed the acceptable load – This is true (mainly) when these are threating severely the network performance [2],[3],[4]. Remarkably from [4] and other sources, a high peak of network traffic does not necessarily lead to congestion until the E2E quality gets negatively affected.

1.1 Network Congestion (NC) Types

The following points summarize some important details regarding NC occurrence. They are referred to in many research studies when concluding on some of the congestion control's methods/ techniques.

There is no literature with a clear statement about the types of NC, but this is indirectly by understanding what is NC basically and how it occurs along with the network behavior over a period of time. And, one curious question could be whether congestion really happens so at global network or the Internet. In fact, technically and logically, a general control system allows to split the networks system into two levels. The top-level is commonly called core or backbone of the networks, which operates reliably on physical infrastructures. The lower levels thought of network providers (NP) or internet services providers (ISP)

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

and related systems. However, global networks (Global Internet) congestion is moved from its core infrastructure (i.e. global Internet backbone) to the links, by using some advanced networking technologies at the backbone level [14],[15],[16].Therefore, ordinary NC as experienced around by end-users, is then alive mainly between different lower networks level's entities – LANs/WLANS and their portal's connection point (i.e. WAN's routers). Hence, different controls systems are customized and applied particularly at these levels in order to ensure good detection, monitoring and removal of congestion (when it occurs) [2],[3],[4],[13],[14].

In conclusion, a network is said congested particularly from the perspective of a user's viewpoint. As proven facts, this is when she/he can notice some decreases in service quality, which result from an increase in network load [2],[4] [14][15].

1.1.1 Network congestion control essentials

In literatures, two particular network congestion's situations are considered in matter of NC control or NC solutions design. They have triggered various research studies; and the obtained possible control or solution systems have been/are classified into two broad categories as discussed afterwards in this paper. The commonly known situation is the network congestion or normal congestion (NC); and the most complex (i.e. by occurrence hidden phenomenon) is the called congestion collapse.

1.1.2 Congestion collapse in brief

Congestion collapse or congestive collapse is simply the case with the worst of situations in congestion event. (Even) during normal congestion period, it can happen as a result of repetitive transmissions in hope of eliminating the effects of packets loss [2],[3],[13],[14]. Thus, such uncontrollable phenomenon has rendered complex the NC problem solving. Just like an extra drop of water into a cup full of water, a congested network (i.e. actually subnet) can fall into a "deadlock" situation due to just few more retransmissions over its links. Therefore, various detection and control methods have been/are designed to assist the management before congestion (e.g. NC avoidance policy), or during congestion period (i.e. NC removal policy).

Based on [14], congestion collapse first happened in 1980s as internet's problem (Gerla and Kleinrock 1980). And, in (Nagle, 1984) study, it was described as a stable condition of network degraded performance triggered by unnecessary packet retransmissions. And it is characterized by a condition where increasing sender rates reduces the total throughput of a network [4],[5],[6],[7],[8],[9],[10],11],[14]. Elsewise the network 'section' (i.e. subnet) gets so congested while actually no new data is entering into network's links [2].

1.1.3 Congestion avoidance overview

NC avoidance is all about the process of preventing congestion to happen. In fact, the network access link is known as primary bottleneck or the basic congestion point for the data flow to and from client-side [14],[16],[17]. And therefore "congestion is unavoidable" [14].[15]. And this is obviously true due to link's size and despite of existing efforts for this purpose (e.g. Packets sizing, data rate/transmission speed control). Thus, a common sense shows that direct monitoring traffic would be the most appropriate management to tackle congestion to its lowest probability of happening.

The early technique to avoid NC was overproviding – i.e. offering too much bandwidth to service's subscriber [14]. However, as noticed by this author and many others, that process/method has contributed instead to fuel up the congestion to some extents. And, in modern practice, "admission control is the tools /method applied in connection oriented network". Whereas, congestion control types (i.e. Close-loop & Open-loop methods/techniques) are for packets networks [2],[6].According to [14], multiple backgrounds based services applications networks like VoIP/multimedia network and the global internet at large would better perform by implementing admission control for solution support, rather than any of congestion control techniques. Hence, in addition to using connections oriented technology into internet backbone, there is an admission control to strongly prevent the intrusion of any severe congestion collapse [2],[10],[14]. Furthermore, a proper congestion control or avoidance solution requires some considerations like:

- ✓ Traffic source: for management initial decisions
- ✓ Network scenario model – i.e. implemented traffic management on the paths
- ✓ Feedback enabled from destination – details (receiving node) conforming service achievement quality.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

- ✓ Basic of the performance goal to be achieved – this refers to the type of application services and thus the expected level of performance, which will define its requirements.
- ✓ Etc.

The above details are few of the most important points of knowledge suggested in [6],[14], which are essential to get started with a NC solution designing or enhancement.

- As a concluding point: admission control (for the backbone of the networks/connection oriented network and congestion control (for packet switched networks/global internet sub-networks) are the two main categories of performance solutions provisioning and the base of PQ/SQ -- performance quality/service quality.

2. NETWORK CONGESTION CAUSES AND DETECTION

Congestion happens as a result of some situations caused either by external facts or uniquely as due to an internal reaction of the network experiencing ordinary congestion phenomenon. Here are introduced some of well-known causes of NC.

2.1 NC Congestion Causes

A network is made up of multiples interconnected small networks (i.e. subnets) that are interacting through routers. Packets flow from one to another (or others) at different moments, with various performance requirements and without the knowledge of when/how or what is taking place on the other subnet. Nevertheless, all the generated packets have to cross a single junction (i.e. routers or Access points elsewhere) at different locations prior to entering or going out the internet toward the receiving nodes. Therefore, for various reasons, traffic congestion can happen either at the level of subnets (i.e. local or borders' router) or network (i.e. edge or WAN's routers). The following are included among the causes for network congestion level.

1) Situation whereby links or nodes carry more data than required and thus compelling edge or endpoint routers to throw any extra of their entering packets [2],[3].
2) Congestive collapse (i.e. temporary Network internal phenomenon due to a congested situation and then auto-set into repeatedly transmitting all the "considered" lost packets): It is believed to be the cause of ever disliked congestion categories/types [2]. That because, it is able to undermine the NC real-causes and thus inducing network managers always into wrong believes about what happened/went wrong and what is still going on.
3) Concurrent TCP or any traffic flow facing port queues buffer tail-drop can degenerate into congestion activity; such congestion is termed TCP global synchronization [2].
4) Subnet's loads deployed into network links and which are beyond acceptable scale of the acceptable and available bandwidth (i.e. beyond data rate & buffers size). Then, the network will experience few congestion variations as illustrated in Figure 1; it shows also the concept behind NC event (i.e. the meaning/interpretation; the normal and abnormal).
5) Burst of packets traffic/Flow over transmission time -- Intuitively defined by [7] as "a group of consecutive packets with shorter inter-packet gaps than packets arriving before or after the burst of packets"; whereas to [8], it is a continuous transfer of data without interruption from one device to another. Overall, burstiness in packets flows is susceptible of causing congestion.
6) Etc.

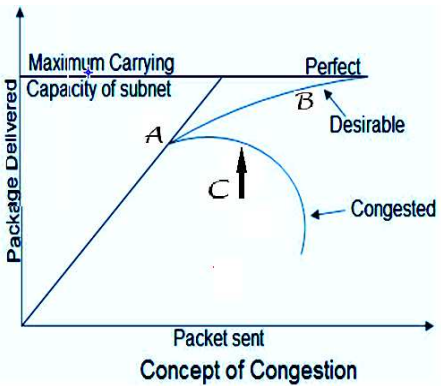

Figure 1 NC through sent vs. delivered packets (Theoretical view)

Figure 1 Legend:

a) "A→B" range – Case data/Packets# exceed the acceptable load of links, but users' observed services quality is still satisfactory;

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

b) "A→C" range – When congestion is intolerable (i.e. including the risks of congestive collapse) – less guaranty for good network performance (A→B shift onto A→C" range), the network is set into actual congestion.

Remarkably based on [4] and other sources, from points (a, b) a high peak of network traffic (case 'a') does not necessarily lead to congestion until the E2E/delivered services quality gets negatively affected [case 'b']. Otherwise, these show that network lives always with congestion, exception in the network backbone where transmissions operate over fiber optic system in most cases nowadays, but not really impossible in WN due to always present waves interference. And thanks to choke-point's router job in limiting into affected links the spread of subnets' congestion onto global networks Figure 2.

2.2 **Subnets Congestion Causes**

Congestion on networks is generally a normal response of the network based on the subnet's client's services request. However, based on various sources including [3][4][6][14], its causes can be due to the following happening:

- Traffic/data rate generated by clients is beyond the link's supported value. Therefore, there is a risk of blocking transmission (e.g. Figure 2) due to router's buffers overloading. Hence, source forwarding line's capability gets weakened – low throughput is observed at end-points. This will be then followed continuously by packets loss because of being discarded/dropped at router's interface (And the source repeated transmissions is at assumption of the previous ones lost);
- Poorly dimensioned router's buffer, including its low processing speed in tasks, management (i.e. bad bookkeeping tasks). And router's buffer with enough space and adapted processor speed to a traffic flow will be just fine to delay the risks of congestion;
- Choke point router not fast in traffic management (e.g. entry/routing tables updating, queues sorting in buffer, etc.). Such systematic matter will naturally hide the root of the congestion. Hence, monitoring the system and choosing a correct computer instead can be a better solution (for this point);
- Links' slowness. But, remember that overproviding link bandwidth is not of best solutions especially with high speed links in use. Instead, give time for router recovering itself. For, packets repeated transmissions can turn normal into worse congestion – say congestive case [4].

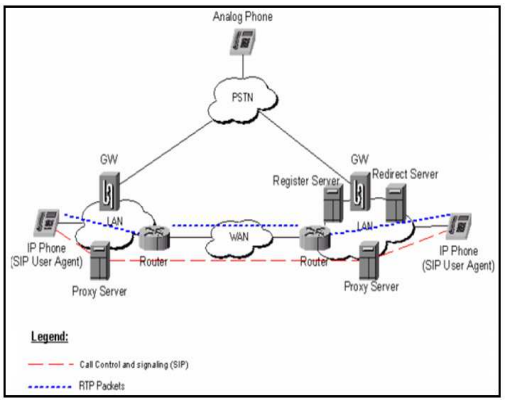

Figure 2 Role of Choke-point (LAN to & from WAN's router) for Congestion control between subnets and global network [5]

Figure 2 illustrates the neutralization of subnet's congestion effects spread onto Internet (WAN) with edge routers' contribution—thus 'NC' felt mainly within subnet user's connections.

2.3 Congestion Detection Strategies

NC detection is likely a proactive process of taking care of a network run, in which some strategies are implemented in order to tell earlier the possible advent of congestion. Here are analyzed some popular detection methods. They aim each at alerting on the congestion occurrence. And, the detecting or controlling mechanisms are either implemented on the network end-node (i.e. sending and receiving terminals & local routers) or on the local networks end-point/interconnecting-point's router called choke-point's routers (i.e. intermediate or edge routers). And choke-point's routers are the networking data-coms converging point of all the links from different LANs/WLANs to be routed over to the others across WANs' environments [2].

2.3.1 NC detection method groups

From ordinary congestion stance, the following discussed mechanisms were designed to successfully handle the network operation when fallen into congestive collapse; or to particularly prevent the congestion from happening. In fact, the following three groups represent broadly the mechanisms category under which several different

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

algorithm have been developed to contribute for this purpose on specific perspective [2],[3],[4]. These are:

a) **Explicit congestion notification** (ECN), an extended mechanism to TCP/IP protocol. It uses a flow control system to proactively enable both the source and end communicating nodes to readily behave as required.
b) **TCP congestion-avoidance algorithm**, a systematic flow control capable to reduce NC and handle it when happened;
c) **Network scheduler**, the most practical method. It is about an actively coding program built into most communications networking routers interface for dealing with traffic active queues management. Based on the coded behavior, it triggers arriving packet discarding/dropping or sorting during congestion period;

These general groups merely tell about the existence of various techniques for congestion prevention. One of the reasons for techniques pluralism is basically because of various network applications services with different performance requirements, which are sensitive to congestion effects. Case examples include VoIP and various multimedia applications; in addition NC influences somewhat differently LANs and WLANs, and thus their managements as well. Therefore, the design of network performance solution support, must account these concerns. For, beyond avoiding NC, there are more importantly the network consumers experience and their satisfaction. It is interesting to realize that congestive collapse is likely the most worried of issues in network performance management, since routers most implemented mechanisms (e.g. QD) are typically for its prevention. Furthermore, the QD (Fair-Queuing particularly) is argued as being the most preferred on 'Choke points' (medium) -- routers interface (RED for large ones) [2]. Therefore, indirectly, all the problems (i.e. networks systems and its applications services performance issues-more spoken nowadays in terms of services quality) are addressed under NC avoidance or just congestion control. Unfortunately solving for congestion collapse is not enough [2],[4]; for, there are particular and preferential performance requirement (e.g. QoS conditions for RTA) cannot be satisfied under this solution perspective – but by integrating few or more algorithms to the task..

3. MONITORING & CONTROLLING CONGESTION

3.1 Overview

Monitoring is about indicating, recording/keeping track of events/phenomenon on a particular problem/issue's aspect in support to action taking for system improvement requirements or, for merely appraising the achieved performance. Example: Amperes and volts indicator devices (i.e. Ammeter, voltmeter) inserted onto an electric energy line to show the consumed value over time. Another example is a pluviometer or barometer in a weather forecast lab indicating and recording temperature and other facts for further analysis. And comparatively, this is what is being done by Congestion-avoidance algorithm. For practical solution example: Discarding policy method applies a technique of favouring only sensitive data traffic; and thus it drops anything below this category. Selected parameter setting enable to sense early signs of congestion (e.g. no ACK received, E2E decrease, data rate increase, latency increase, etc.) [2],[3],[4],[6],[14].

As a particular remark, monitoring mechanisms action is a proactive based algorithm for congestion events; it permanently attempts to detect, then deviating sooner the cause that is able to end up into a congestion situation.

Controlling is instead about a system comparator for gauging and immediately taking action whenever a given parameter level (i.e. standard/selected value) has been reached over an operation time of the system containing it. That is the job model done by a network scheduler (i.e. by enabling router, end-node terminal/AP to drop packets in congestion time). In networking practical solution example: "explicit congestion notification / ECN" uses a flow control system information [~~but~~] to notify simultaneously the senders and end receiver sources to actively take required action on NC event going on [2],[3],[4].

And contrary to monitoring algorithms action, controlling system/mechanism action intervenes only at the congestion time; otherwise it is a reactive based method to congestion events.

3.2 Practical Methods

An attempt to shade lights on which could be their difference is illustrated in precedent paragraphs. And, NC controls methods can be seen as techniques or mechanisms based on a set of policies implemented as preventive or

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

curative/active strategy against congestion occurrence.

Basically, they are of two categories, namely open and closed loop congestion controls. Respectively the first is implemented to avoid (or push back and minimize) in advance NC from occurring; whereas the second acts like fire-fighters –i.e. stopping congestion after it has occurred [2],[3],[4]. Referring to above section, one can now easily see which of indicated methods would work better for controlling or monitoring upon reading their further explanations provided next.

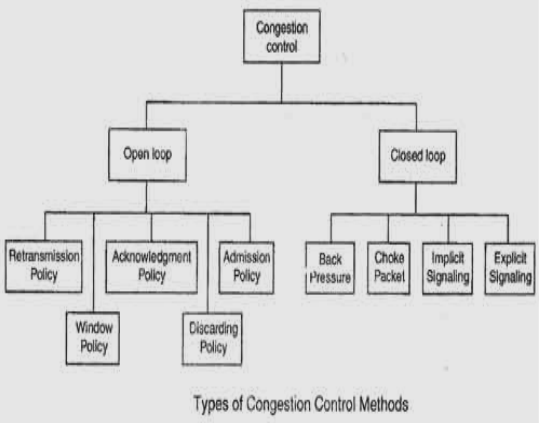

Figure 3 Controls Common Methods [4]

Figure 3 exposes the two congestion control categories and their respective policy members.

3.2.1 Case **for open loop policies**

Set of five policies based techniques (Figure 3). A glance on the group members discloses/tells about the elements supporting/enabling them to monitor facts in the subnet and skip possibly congestions. For example, methods policy such as:

- ✓ ***Admission policy*:** router's intelligence enables to not set on virtual links in case of risk probe for congestion soon or afterwards, and even ignoring the network switch's approval for resources status for new flows. And [4] described this strict rule as quality-of-service mechanism (referring mainly top RTA;
- ✓ ***Window policy***: applying 'selective reject window' instead of 'Go-back-n' methods can minimize possible packets duplication that favours congestion worsening. Because 'Selective reject method' sends a request uniquely for clearly missing or corrupted packets, warranty for no (or worse) congestion.
- ✓ ***Retransmission policy*** – in cooperation with some or either above policies, its potential is maximized by accounting retransmission timers during system design /configurations;
- ✓ ***Acknowledgement policy*** – ensures very fewer chances for links overloading with ACK to be initiated by receiving nodes or, attached it to traffic load; including other option like: issuing it after receiving n-packets or when timer-out.
- ✓ ***Discarding policy*** – targeting mainly less sensitive services traffic is an advantage to secure services quality where repair is difficult (voice, videos based application, etc.); including keeping the network integrity.

3.2.2 Case for closed loop policies

Acting in a fire-fighters group manner, this method involves 4 techniques each shortly described in next lines.

- ***Choke packet technique***

Routers implementing it will issue during congestion moments a called "choke packet" (in warning) to the line point that is in congestion event. And in turn (and as method limitation), the warned node cannot alert/share this message with all those through which it got the data creating congestion but, only the actual data source/sender.

- ***Backpressure technique***

As the name shows, it operates in flushing the surplus of the data from the congested node back through all its precedents until reaching the sender of these extra packets on the line. Hence its nickname node-to-node controls system [4].

Remarkably, this technique holds simultaneously two great actions. That is removing the congestion from congested point; and preventing any downstream nodes while going through each one till the origin. This is likely more secure than choke-packet solution, but it may take longer time going through all backward nodes

- ***Explicit signalling***

This means that when an endpoint has received some packets triggering a congestion event, it will transmit directly a warning message to its origin sender.

Unlike choke packet technique, this one can set an intervention /action (i.e. Signaling) in either directions from congested point.

For a forward intervention progation (i.e. toward the destination), the packet's receiver will receive also a message attached to a packet and requesting this terminal to delay sending the acknowledgement. As to backward intervention a

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

warning signal is sent to the source asking to reduce it sending rate or speed. [4],[14]

As lesson, the source being alerted on congestion happening on the line – (nackward signaling message) including a Zero-claim for packet lost through ACK message—stopped with forward signaling to destination: therefore possible packets duplication (i.e. claimed/assumed to be loss replacement) is eliminated. Method quite great/ more efficeient provide the two direction signalling confifiguration enabled and works fairlry.

3.3 NC Control Methods Summary

Based on [9],[10],[11],[12],[15], here are some commonly used methods in NC management.

- **Network congestion control-**The mechanism is similar to end-to-end flow controls, but only to reduce congestion in the network, excluding in the receiver.
- **End-system flow control** —just to prevent the sender from overrunning the buffers of the receiver.
- **Network-based congestion avoidance** — lets a router sense the congestion and attempts to slow down senders.
- **Resource allocation** —this set on a virtual circuit, across a series of switches with a guaranteed bandwidth as resource allocation.

These above mentioned are general mechanisms; and specific techniques (e.g. queuing disciplines in VoIP based application) can be used in some situations (e.g. SP networks, corporate/campus networks, etc.;) requiring particular treatments in order to produce the expected performance. Such cases may involve either of the following:

- **Queuing --** Buffers on network devices are managed with various queuing techniques. And, properly managed queues can minimize dropped packets and network congestion, as well as improve network performance.
- Congestion control in frame relay — implements two congestion avoidance mechanisms: BECN **(**backward explicit congestion notification**)**, And FECN **(**forward explicit congestion notification**)** [12],[16].
- **Congestion Control and Avoidance in TCP** — designed to prevent overflowing the receiver's buffers, not the buffers of network nodes.
- **Slow start congestion control** — a technique tha**t** requires a host to start its transmissions slowly and then build up to the point where congestion starts to occur.
- **Fast retransmit and fast recovery** — algorithms designed to minimize the effect that dropping packets has on network throughput.
- **Active queue management** (AQM) **--** a technique in which routers actively drop packets from queues as a signal to senders that they should slow down
- **RED** (Random Early Discard) – one of active queues management (AQM) scheme uses statistical methods to drop packets in a "probabilistic" way before queues overflow.
- **RED** makes two important decisions: when to drop packets and what packets to drop. It makes packet-drop decisions based on two parameters – minimum vs. maximum thresholds.
- **ECN** (explicit congestion notification) **—**a technique applicable in congestion avoidance mechanism [4],[16] ;
- **TCP rate control –**It often referred to as ERC (explicit rate control),

Other Specific schemes:

- Additionally to general methods introduced earlier, to manage network traffic beyond what those schemes provide, you need to look at other ways such as prioritization schemes, packet tagging schemes, virtual circuit schemes, and QoS schemes –very important for wireless Network (WN) and especially multimedia based service applications [12].

- **Implicit signalling:** with this technique configuration, there is no messaging information from congested node to (or from) the packets source and other nodes in the line. Instead, the source “intuitively” learns about the congestion from the lack of expected feedback from the packet’s destination. Therefore, the sender automatically reduces its packets transmission rate (Slows down). Implicit signalling is similarly implemented in TCP mechanism for this purpose [4].

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

3.3.1 Case for congestion monitoring

From above diagram (Figure 3: Controls Common Methods), none of congestion control methods is only for monitoring activity. However, some of methods act using techniques operating on basis of tracking facts (i.e. monitoring). For example admission and discarding policies are of this type. And in else cases, there is a need for information forecast through facts tracking in order to predict and thus prevent a complex event like network congestion collapse. Therefore, open-loop congestion control methods can be then be seen broadly as "monitoring" procedures based congestion control. Moreover, under these policy categories some methods actually make use of other's component feedback (i.e. ACK) or locally observed facts to make decisions.

Otherwise there is always a need of cooperation between those mechanisms I order to bring about more powerful control strategy and thus better performance /service quality. Hence, integrated mechanisms based solutions for networking management is a way for network performance with less congestion. And this is sufficiently good for the current and future of networks trend (i.e. mobile & multimedia based networks deployment & contents); even though solving for NC/congestion is said to be not enough [2],[4], it is actually worth for containing almost all the ingredients for service quality basic, especially conditional QoS/MMWN QoS (i.e. the QoS with leading conditions for performance acceptance or evaluation in the current and future networks model). It is then only a matter of configuration considerations and few more twists in design process to suit some specific conditions as requirements in critical/sensitive applications performance.

3.3.2 Case for congestion controlling

Here goes a similar remark like in 'monitoring' case. In fact, this introduction showed that congestion management applies some cooperative efforts within each method's framework. Hence, with a focus on some particular performance's requirements, some methods are likely for controlling or monitoring network's traffic. In generally, "control" is the most used terminology, and practically it includes the activity of monitoring.

4. SAMPLE ALGORITHMS FOR CONGESTION

Sample considerations made for congestion control algorithms categorization has been studied in [2] and that based on:

- ✓ The type and network recorded amount of feedback (e.g. Loss; delay; nature of explicit signals).
- ✓ Deployment credential throughout/across the networks --for instance: configurations/settings are required uniquely on sender/receiver/router's interface, or on both "sender & receiver's interface (router case exclusive)", and then on altogether "sender & receiver & router interfaces at a time". The level of authorization on the networks administration plays important role in this class/category;
- ✓ Applicable conditions and level of fairness—i.e. high/low/medium; maximum/minimum etc.
- ✓ Important considerations and priority choice in improvement level to quality achievable (e.g. bandwidth-delay; fairness, lossy links; short flows prioritization; links data rate level; etc.) [2].

5. WIRELESS NETWORK CONGESTIONS & REASON FOR RECONSIDERATION

5.1 Need for NC Further Considerations

Based on this articles review paper, here are few observations taken as assumptions for the need of reconsidering and learning to better understand congestion as inseparable part of network behaviors of all the time and probably until future generations of the network. These observations become more interesting when switching the vision into the possible coming changes based on the current networks deployment model, including the user's learning and experience on ICT applications.

(Assumption 1):

Normal NC has been in experience since data communications network birth. It has triggered over time the ideas of various ways of improving both the communication network and its application services. However, a comparison between the explanations on normal congestion and on the-called congestion collapse (section 1.2) showed that NC is an inherent part of the commutations

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

networks' behavior of before/past, then now/today and probably in future time.

(Assumption 2):

Prior to 1980s, there were no ideas about congestive collapse, but NC of course. By middle of 1980s it got a first acknowledgement as being a cause of severe decrease throughputs during congested situations [14]; and few more years after the first solution was born (1987), then others followed until nowadays [2]. Therefore, more research efforts might be always needed to get rid (or better say' to curve to the possible lowest levels) or just to minimize the advent of congestive collapse.

(Assumption 3):

A glance at NC Ctrl algorithms categories (introduced here in section four) shows that there are at least four groups [2]; and the various reasons supporting this classification are somehow a proven fact that no single solution algorithm would dare alone in solving enough for these different backgrounds of issues on network and services performance through NC (as problem generic).

(Assumption 4 as concluding point):

From all above discussions, congestion in fact, is the bottom point of almost all sources of network performance problems, which are much presented nowadays in the name of QoS performance complains. Referring to Figure1, NC holds/has all the influencing elements for services quality (QoS) put onto claims in matters of performance experienced below expectation. Otherwise, congestion contains the root of all such blames due to either of the following consequences.

a) E2E not reached means discarded or /and finally lost;
b) Less delivered packets are referred to as poor throughputs under various defects observed in cases for instance of all RTA, multimedia and mainly voice /video applications;
c) Data late delivery can distort the message quality including disgusting its user at receiving ends (e.g. Voice in phone calls, video & audio materials).
d) Etc.

Overall, these statements are frequently expressed nowadays much more in terms of services quality (QoS). In agreement with reviewed NC articles, there is a perceived endless congestion related problem to always face and thus requiring new efforts from researchers and network developers. This is all about increasing more of the network's services application and the ever growing efforts in improvements for both the network's technologies and user's demands of services features. Therefore, delivering an adequate QoS in today and future generations of network can be obviously only through the implementation of multiple mechanisms based integrated solutions method.

5.2 NC Literature Review Particular Remarks

Network congestion issues can be seen as in line with the growth in technologies innovation, services application features and network performance demands. And according to [14], some years ago (and more in future years), the networks will be applying massively overprovisioned core to curve down NC effects. Yet this *has been* /is/will be *made possible with more powerful technologies (*e.g. GB/10GB Ethernet, optical networking, and UMTS systems). However, as (positive) consequence, the traditional network congestion has shifted from the core to link congestion, but with same aim. In network literatures, they use "high performance networks" or "high speed communication" phrases to point at this new ways for NC management.

However, further great reasons for giving more consideration to congestion in coming years of networks can be learn out of this statement from [14]: "*Congestion control is about using the network as efficiently as possible. These days, networks are often overprovisioned, and the underlying question has shifted from 'how to eliminate congestion' to 'how to efficiently use all the available capacity'. Efficiently using the network means answering both these questions at the same time; this is what good congestion control mechanisms do"*.

Finally, since recent years the tendency for networks with more multimedia applications content is telling implicitly about such situations of overloading links, thus congestion of network in future years.

5.3 Article Particular Contribution

This is shortly a discussion about why congestion can be considered for today and future networks. It deserves receiving more concerns basically because of continuous growth of network's technologies to suit user's more demanding features. In fact, as far as we want to connect more people with more multi-background services and with faster speed as possible, there will be always a probability of congestion in the "air" or virtual links (i.e. magnetic waves environment) or in the physical links (wired sides). In other words, congested network is directly subjected to user's

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

wants over it and thus its utilization level according to users desired amount of services in request making up the called link-load at a particular time. Hence, the advancement in network technologies and the increasing awareness of people knowledge in IT/ICT capabilities do not show yet a hope/reason for turning downward its (currently growing) learning curve. Therefore, engineers will learn more to cope with congestion rather than expecting to get rid completely of it.

And as future work, network congestion control will be studied and analyzed on LAN/WLAN simulations environment, implementing some of the commonly control methods for both exploration and verification of most theory's statements. This will include some scenarios for multimedia network performance's comparative study, with alternatively implemented former NC solutions and then some typical ones for multimedia applications. Hence, to learn about the solution effectiveness with respect to the network content change.

6. CONCLUSIONS

Here is the end of this articles review paper, which has attempted as much as possible to cover the key points stated at the introduction (i.e. Abstract). With a hope that its content can serve for the purpose express also earlier, the future work will be undertaking a series of simulations testing in order to closely witness all theoretical detail discussed in this article.

ACKNOWLEDGEMENT

We would like to acknowledge the support of the Universiti Teknikal Malaysia Melaka (UTeM) for the journal publication fees funding, and to thank all the friends and colleagues for their helpful comments and encouragements.

REFERENCES:

[1] Sandrine, Anonymous, 2015 *Network Congestion Management: Considerations and Techniques; An Industry Whitepaper, Intelligent Broadband Networks, Copyright ©2015 Sandvine.*

[2] LINFO, 2005 *Network Congestion Definition*; available at: [http://www.linfo.org/congestion.html]. Copyright © 2005 The Linux Information Project'

[3] Webopedia, anonymous, 2015 *What is congestion? A Webopedia Definition; Networking*; Available at: [www.webopedia.com];[https://www.techopedia.com/definition/18506/congestion-networks]; Copyright ©2010 – 2015; Janalta Interactive Inc.

[4] E-Computernotes.com, Dinesh Thakur, n.d. *What is Congestion Control? Describe the Congestion Control Algorithm commonly use*. Available at: *[ecomputernotes.com/computernetworkingnotes/...networks/]*.

[5] Minacom.com, anonymous, 2005 *VoIP Technology overview*, Service level test Authorization. Minacom; ©2005. All right reserved.

[6] Sandvine.com, *Network Congestion Management: Considerations and Techniques*. Industry Whitepaper;

[7] R. Krzanowski, 2006 *Burst (of packets) and Burstiness*; 66th IETF - Montreal, Quebec, Canada; V1.0;7/10/2006

[8] Linktionary.com, Tom's Sheltom, 2001 *Burst and Bursty Traffic,* Telecommunications and networking Encylcopedia; Available at: [http://www.linktionary.com/b/burst.html]. Copyright (c) 2001 Tom Sheldon and Big Sur Multimedia. All rights reserved under Pan American and International copyright conventions.

[9] Darus Butinas, 1995…*Congestion Control*; Available at: [http://www.cs.wustl.edu/~jain/cis788-95/ftp/tcpip_cong/].

[10] Vern Paxson Dilip Antony Joseph and Sukun Kim, 2006 TCP Congestion Control- EE 122: Introduction to Communication Networks; Fall 2006 (MW 4-5:30 in Donner 155).

[11] Stefan Savage, (Lecture 15) – Congestion Control, CSE 123: Computer Networks (course); UCSD (University of California, San Diego).

[12] Linktionary.com, Tom Sheldom, 2001 *Congestion Control Mechanisms;* Description of Congestion Control Mechanisms from Tom Sheldon's Encyclopedia of Networking and Telecommunications. Copyright (c) 2001 Tom Sheldon and Big Sur Multimedia. All rights reserved under Pan American and International copyright conventions.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[13] University of Southampton, S. Chen, n.d. ELEC3030 (EL336) *Computer Networks*, Lecture, Electronics and Science. University of Southampton.

[14] Michael Welzl & Leopold Franzens, 2005 Network Congestion Control Managing Internet Traffic, e-book; Copyright © 2005 John Wiley & Sons Ltd, The Atrium, Southern Gate, Chichester, *John Wiley &Sons, Ltd.*

[15] Tech Mahindra, Vivekanand Tiwary, n.d. *Congestion Control in 4G Mobile Networks* –A Business Imperative; Connected World, Connected Solutions; Tech Mahindra Technical Paper; Available at: [*www.techmahindra.com/.../CongestionControl_4G-Newo*]

[16] Seamless Congestion Control over Wired and Wireless Networks; Available at: [www.aueb.gr/users/.../s23]

o