Computer Communication & Collaboration (Vol. 3, Issue 3, 2015)
ISSN 2292-1028(Print) 2292-1036(Online)
Submitted on Apr. 6, 2015
DOIC: 2292-1036-2015-03-001-55

Dynamic Regulation of Cross Traffic in Wired IPv6 Networks

Mahamat Hassan Borgou

Institute of Science and Technology of Abeche (Tchad)

mahamatborgou@yahoo.fr

Cheikh SARR (Correspondence author)

Faculty of Science and Technology, University of Thies (Senegal)

BP 967, Thies Senegal

csarr1979@hotmail.com

Abstract: In this paper, we propose a new protocol named Regulation of Cross Traffic (RCT) which supports Quality of service (QoS) throughput guarantees and provides a distributed regulation mechanism for cross traffic in wired IPv6 network. By adapting dynamically the rate of cross traffic among the network, RCT increases the acceptance ratio of QoS flows and provides a good use of the remaining resources through the network. Our protocol also provides an accurate method to evaluate the available bandwidth in wired IPv6 networks which is able to differentiate QoS applications from cross traffic. Through extensive simulations, we compare the performance of our proposal scheme with some others protocols to show the improvement.

Keywords: Quality of Service, Cross Traffic, Available Bandwidth Estimation, IPv6 Networks

1 Introduction

Internet Protocol version 6 (IPv6) [4] is the next generation Internet Protocol designed to be the successor to version 4 (IPv4). IPv6 provides new features, for instance, expanded addressing, simplified header format, improved extension, and option support [6]. These new features also integrate Quality of Service (QoS) mechanism to offer applications better performance. QoS focuses on several metrics, like delay, bandwidth, loss probability, etc. Our proposed scheme focuses on the bandwidth parameter which is an important metric often used to perform admission control, flow management, or congestion control in wired networks. We assume that two types of applications are transmitted in the network:

- The first one requires guarantees on their throughput, like, video transmissions. They are called ***QoS traffic*** henceforth.
- The second one is more tolerant to changes on their throughput, like, file transfer or web traffic. They are called ***cross traffic*** or ***best effort traffic*** henceforth.

Several existing approaches focus on the guarantee of bandwidth for QoS traffic without dealing with cross traffic. Most of these works in this area supply guarantees for QoS flows, thanks to an evaluation of the available bandwidth. However, these evaluations do not provide any differentiation between QoS and cross traffic data packets. This lack of differentiation may lead to situations where there is not enough available bandwidth for a new QoS traffic just because most of the bandwidth is already occupied by cross traffic. Such approaches limit the number of accepted QoS flows.

In this article, we provide a new QoS mechanism called Regulation of Cross Traffic (RCT), which can regulate dynamically the throughput of cross traffic (when it is necessary) and provides throughput guarantees to QoS flows, according to an evaluation of the available bandwidth. This evaluation mainly relies on the capability for router to estimate the link occupancy and so on the available bandwidth on a specific link as described in ABv6 (Available Bandwidth for IPv6) already presented in [5].

The regulation scheme of RCT proceeds in two phases: decreasing the throughput of cross traffic in order to increase the number of accepted QoS flows and increasing the throughput of cross traffic to provide a maximal use of links when it is possible.

The rest of the paper is organized as follows: Section 2 presents related work. Section 3 presents succinctly the different mechanisms used in RCT. Section 4 describes our regulation protocol RCT, and finally, simulations results are presented in Section 5.

2 Related work

To offer throughput guarantees to QoS flows, routers need first to evaluate the amount of bandwidth that is available in the network to ensure that the resource requirements of QoS admitted flows can be handled by the network. Different solutions have been proposed to evaluate the available bandwidth. These solutions have generated several contributions in the wired networks communities. They can be classified into two major categories:

The **active approaches** [3, 7, 2, 9] techniques rely on the emission of dedicated end-to-end probe packets to estimate the available bandwidth along a path. Generally, two or more packets are sent together in varying configurations and use the relationship between the packets to determine the network bandwidth. These packets can be sent in pairs of equal or varying sizes or as a train of packets.

The **passive approaches [**11, 5**]** techniques use only local information on bandwidth utilization. The typical example of such approaches is a router monitoring the link utilization. These mechanisms may exchange information via one-hop broadcasts. This exchange can be done through Hello messages used by many routing protocols to discover the local topology. As long as these exchanges are not too bandwidth consuming and integrated into the routing process, such measurement could be considered as passive technique.

These different estimations are then used in a routing protocol in order to compute QoS routes, i.e., routes that offer at least the requested bandwidth. These works mainly focus on the QoS traffic and do not optimize the cohabitation between QoS flows and cross traffic flows.

To sum up, none of the described protocols in this section takes advantage of the differentiation between traffic to provide an accurate regulation mechanism. In this work, we start with ABv6 that is, from our point of view, the most accurate protocol so far for evaluating the available bandwidth on a link, which is important for guaranteeing throughput. Then we add a differentiation mechanism to ABv6 in order to provide a more efficient bandwidth management.

3 ABv6

For ensuring cross traffic regulation, our solution relies on accurate available bandwidth estimation. We choose the protocol ABv6 proposed in [5]. The author shows that ABv6 is more accurate than several protocols with the same goal while requiring a small overhead. By considering the overlapping of the silence periods of both emitter and receiver routers of a link, ABv6 reaches accuracy in the estimation that is often not achieved by the other protocols. IPv6 extensions are also used to compute a protocol version.

As our regulation mechanism depends on this available bandwidth estimation, this section is devoted to the description of ABv6. Of course, due to space limitation, we cannot include all the details of ABv6 that is not the novelty of our proposition. The interested reader can refer to [5]. For providing an accurate evaluation, some phenomena need to be taken into account:

The link utilization has to be monitored to evaluate the capacity of a router to emit a given traffic volume. This link utilization is computed by each router by monitoring the traffic over the link and measuring the total amount of time that is idle.

For a transmission to take place, both routers emitter and receiver need that no jamming occurs during the whole transmission. Therefore, the value of the available bandwidth on a specific link depends on both peers' respective link utilization ratios but also on the idle period's synchronization. In [5], we propose a probabilistic method to estimate this synchronization. This estimation, for the link (s,r), is denoted $E(b(s,r))$ in the following ($E(b(s,r))$ is the available bandwidth for the considered link (s,r)).

ABv6 introduces some modifications on the usual Hello packets to take into account the bandwidth measurement and carry out a protocol version. The protocol uses IPv6 extension to disseminate bandwidth information in the neighborhood.

To sum up, on ABv6, on a link (s,r) where t_s is the link utilization around the router s and t_r the link utilization around the router r, the available bandwidth on this link denoted by $E(b(s,r))$ can be computed with the following formula:

$$\boxed{E(b(s,r)) = t_s . t_r . C}$$

where C is the capacity of link (s,r)

4 RCT: a dynamic regulation cross traffic protocol

This section describes how we introduce the differentiation in the available bandwidth estimation and how we use this estimation for a regulation of cross traffic. The first step is the differentiated estimation of the available bandwidth. It will allow us to quantify the proportion of the available bandwidth which is occupied by QoS flows only. This estimation relies on the protocol ABv6 (Section 3). However, in the current state, ABv6 is not able to differentiate between QoS and cross data packets. Therefore, we present hereafter how we perform this differentiation in order to enhance the measurement accuracy.

4.1 Differentiation between QoS and cross traffic

As explained previously, a differentiation between QoS and cross flows allows a better use of the available bandwidth for new QoS transmissions by reducing the amount of cross traffic. We assume that each packet is marked in its IP header in order to know to which kind of flow it belongs, i.e., a QoS flow or a BE flow. Packet marked with 1 belongs to QoS flows otherwise packet marked with 0 belongs to cross traffic flows. The marking process is done at the "traffic class" field of the IPv6 packet header. Indeed, this field is used for differentiated services, which is useful to classify packets.

The differentiation in the remaining bandwidth estimation is simply done at the link layer and consists in measuring only medium occupancy of QoS data packets (ignoring cross traffic) during the monitoring phase of ABv6.

To summary, each router computes its differentiated remaining bandwidth by removing the bandwidth consumed by QoS flows. Then this differentiated remaining bandwidth per router is used to compute the differentiated remaining bandwidth per link denoted D_{diff} with the ABv6 method.

4.2 Regulation of cross traffic

The previous differentiated available bandwidth estimation is not enough to provide guarantees to QoS flows. The cross traffic needs also to be regulated. In RCT, the regulation scheme concerns only the cross traffic. This regulation is done in two steps:

Decreasing the throughput of cross flows when a new QoS flow wishes to be transmitted and does not find enough available bandwidth because this one is partially consumed by cross transmissions. Increasing the throughput of cross flows when a QoS flow reduces its bandwidth or stops its transmission area.

This regulation is coupled with a routing protocol in order to benefit of signaling packets to disseminate information required for our regulation mechanism. We have slightly modified OSPFv6 [1] in order to transform it into a QoS protocol, called RCT henceforth. OSPFv6 is coupled to a reservation scheme like for instance RSVP [10] to inform and to find adequate (constrained) routes for QoS flows.

4.2.1 Reduction of cross traffic

In this section, we explain how we decrease the throughput of cross flows. The regulation process of cross traffics is triggered when a new QoS flow asks to be accepted in the network. Therefore, the search of an adequate route for a QoS flow is intimately linked to the possible regulation of some cross flows. To do this, RCT does not introduce additional message overhead but uses classical route reservation (RRES) and route reply (RREP) packets found in RSVP. Every time a new QoS flow wants to transmit data, it checks the resources availability using these RRES and RREP packets. The information stored on these packets with RCT are:

The throughput requested by the new QoS flow denoted D_{QoS}

The number of cross flows (nb_{cross}) among the path on which the QoS flow is transmitted. For this, each cross flow has a single identifier propagated on Hello messages. Therefore, each router can be able to know the number of cross flows in its vicinity by analyzing these identifiers

The differentiated remaining bandwidth (D_{diff}) which only takes into account the QoS transmissions as described in Section 4.1

The RRES packet contains, in addition to the fields described previously, the IP address of the sender, the destination IP address, and a sequence number. The sequence number is used in order to avoid cycles in the routing process; therefore, a RRES is just examined during its first passage. Each intermediate router that receives a RRES performs an admission control by simply comparing whether the bandwidth requirement D_{QoS} carried in the RRES packet is lower than the differentiated available bandwidth of the link D_{diff}. If it is the case, the router updates nb_{cross} and D_{diff} (if necessary) and forwards the RRES. Otherwise it discards it. nb_{cross} is incremented at each router by the number of cross flows that the router knows. If the differentiated remaining bandwidth of the router that receives the RRES is lower than the differentiated remaining bandwidth given in the RRES, then the router modifies this field with its value. It allows us to know the available bandwidth computed along a path when considering only QoS transmissions (when possible).

When the destination receives a RRES, it also needs to do the checking procedure as described above. Finally, the destination sends a unicast RREP to the initiator of the request along the reverse path to ensure that routers along the reverse path are still reachable. Every time a cross sender intercepts a RREQ or a RREP, it checks whether there is enough available bandwidth to carry the QoS flow without degrading it, by comparing its own throughput (T_{cross}) with the parameter AvailableBandwidth denoted AB computed as:

$$AB = \frac{D_{diff} - D_{QoS}}{nb_{cross}} \qquad (1)$$

If it is not the case, it reduces its throughput by activating a leaky bucket algorithm at the Link Layer (LL) level, on the cross packets with a rate corresponding to the AvailableBandwidth value. Equation 1 computes the new available bandwidth allocated to the cross traffic if the new QoS flow is accepted.

In fact, to set up the reduction scheme, two virtual queues are used at the link layer level of each router. The first queue conveys QoS data while the second one conveys cross data packets. Therefore, we can control dynamically the size of each queue. Reducing the throughput of the cross traffic is simply done by reducing size of the virtual queue affected to cross traffic. It is obvious that to maintain the throughput under a threshold, the size of queues should be also kept under a predefined threshold. Figure 1 represents the internal architecture of a RCT router.

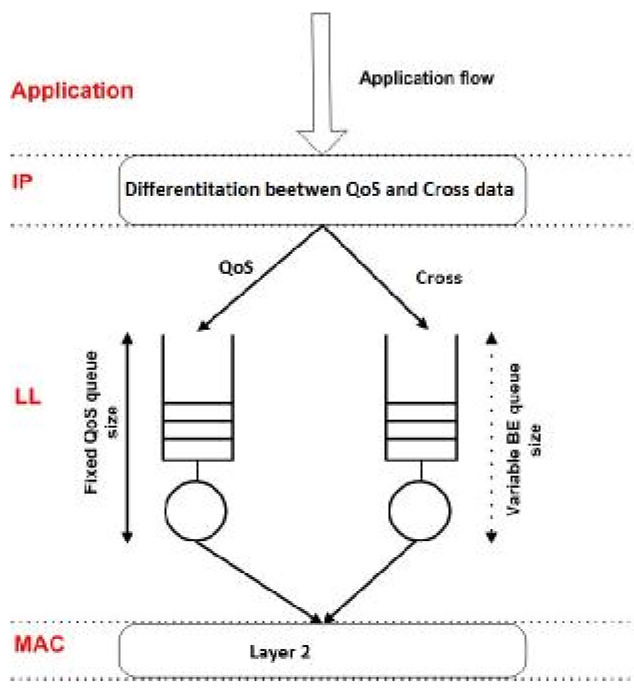

Figure1. Internal architecture of a RCT router

According to Equation 1, a threshold larger than one indicates that the throughput of cross flow is higher than its allocated bandwidth and that a reduction is necessary. Once the threshold is computed, the size of the cross queue is fixed dynamically by computing the ratio between the number of cross packets entering during a window of one second divided by this threshold.

4.2.2 Increase of cross traffic

When a QoS flow stops transmitting or reduces his throughput, all the cross flows that have reduced their bandwidth should increase their throughput in order to use the maximum of the available bandwidth when possible. This value should not exceed the initial value of the cross flow. To address this issue, router monitors the utilization of the virtual QoS queue. When this utilization decreases, routers begin to increase cross traffic as specified.

5 Simulations

In this section, we evaluate the performances of RCT and compare it with other approaches. We use the network simulator 2 (NS-2.35[1]). We compare the performance of RCT with ABv6 to show the improvement of a differentiation mechanism and with OSPFv6 as baseband routing protocol.

To evaluate the different protocols and illustrate the effectiveness of RCT, we generate random topologies with random constant bit-rate flows (random source, random destination and random throughput with fixed 1500 bytes frames). For each of these protocols, similar scenarios (same number of routers and same number of flows) lead to similar behaviors. Hereafter we only analyze two specific scenarios. For each scenario, the results presented here were obtained over 30 simulations runs with different random seeds.

5.1 A simple network

We create a network composed by a single 7-hop path connecting two hosts A and B and composed by 6 routers as shown in figure 2. Cross traffic at each hop is modeled using a Poisson process with packet size determined by an exponential random distribution with a mean packet size of 1500 bytes. The mean rate of the cross traffic flows ranged from 2 Mbps to 4 Mbps at each hop. The number of cross traffic flows is ranging from 0 to 20 at each hop. The link capacity at each hop is also set to 100 Mb/s and each simulation lasts 500 seconds. Host A wants to send two flows (flow1 and flow2) at the rate of **15Mb/s for flow1** and **25Mb/s for flow2**.

The purpose of this experimental setup is to compare the capacity of RCT to decrease bandwidth of cross traffic in order to admit both flow1 and flow2 without throughput degradation.

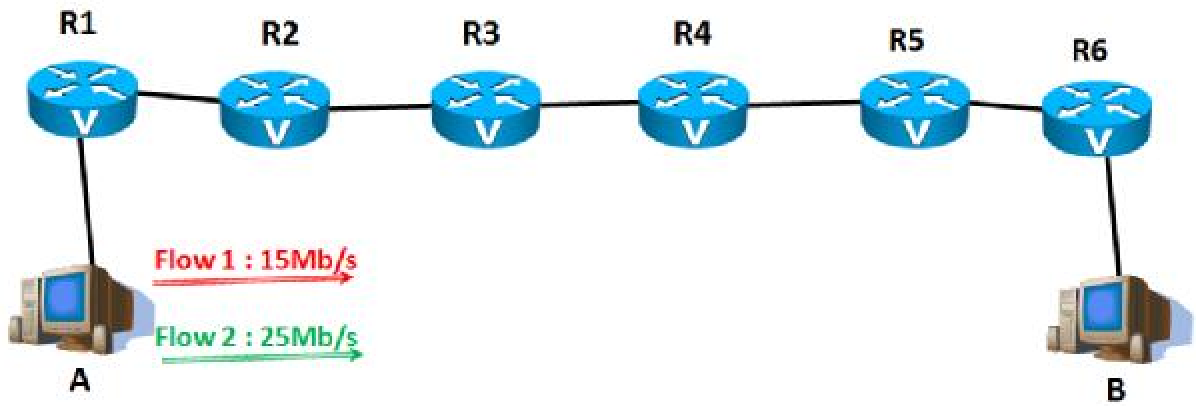

Figure 2. A simple network

1 http ://www.isi.edu/nsnam/ns/

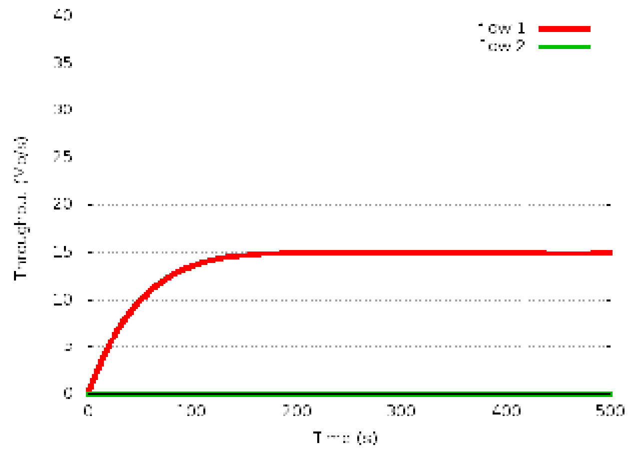

Fig 3(a): ABv6

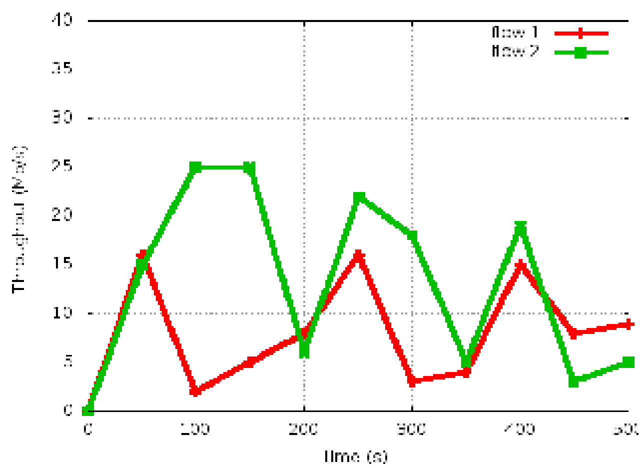

Fig 3(b): OSPFv6

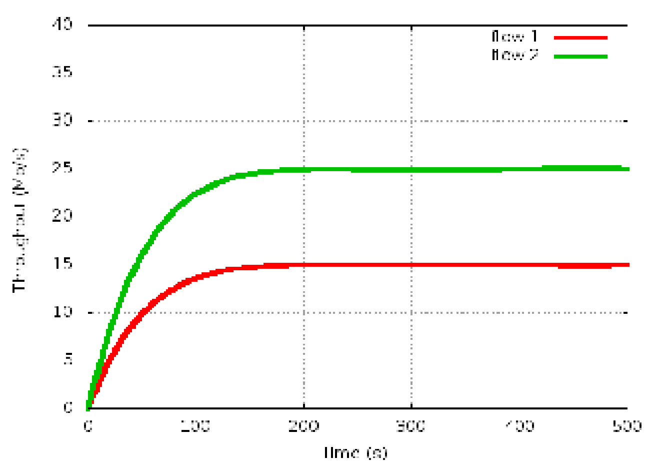

Fig 3(c): RCT

Figure 3. Throughput of flow1 and flow2 with ABv6, OSPFv6 and RCT

Figure 3(c) represents the evolution of the throughput of the two QoS flows obtained with RCT in function of the simulation time, while figure 3(a) and 3(b) shows the same result for respectively

ABv6 and OSPFv6.

When OSPFv6 is used, as shown on Figure 3(b), each QoS connection tries to send its data packets when possible without any regulation mechanism and available bandwidth estimation. This situation leads to a shared medium between the cross and the QoS flows. The throughput of the two QoS flows is consequently degraded.

When ABv6 is performed (Fig. 3(a)), the admission control step estimates that there is not enough available bandwidth to carry the second QoS flow (flow2) with its bandwidth requirement while the first one has successfully been admitted. Hence, only flow1 is transmitted without degradation.

Finally, RCT reduces effectively the throughputs of the cross flows over the path between A et B so that the two QoS flows can be achieved with their bandwidth requirements of 15 and 25Mb/s respectively without any degradation as show on Fig 3(c).

5.2 Random topologies

Let us now investigate the general case. To reflect the accuracy of the cross traffic reduction done by RCT, we define a new metric accounting for the number of right admissions. A right admission happens when the admission control process allows the routing of a QoS flow and this flow's throughput is not degraded by more than 5% when it gets transferred. This definition implies that the differentiated available bandwidth estimation and the reduction of cross traffic throughput are both reliable. The metric we represent hereafter is defined by the following expression:

$$j = \frac{Number\ of\ right\ admission}{Total\ number\ of\ flows} \qquad (2)$$

A falsely admitted flow either degrades the throughput of cross traffic or is not able to achieve its desired throughput. Hence, the value of φ decreases. So φ is able to characterize as well an under estimation as an over-estimation of the available bandwidth among the network.

To compare the different protocols and illustrate the effectiveness of RCT to provide a better regulation mechanism, we measured the value of φ by simulation on a large network composed of 50 routers. The routers are randomly placed. The medium capacity is set to 100 Mb/s. The number of flows ranging from 10 to 50. The throughput of each flow is uniformly drawn between 256 Kb/s to 2 Mb/s. Each simulation lasts 500 seconds and randomly chosen pairs of routers try to establish connections towards random destinations.

Figure 4 represents the values of φ for OSPFv6, ABv6, and RCT in function of the number of QoS flows in the network.

When the network is not too dense (between 10 and 20 flows), the acceptance ratio of RCT is high (about 70 to 80%) while this value is lower for ABv6 (about 40%). Therefore, the differentiation between QoS and cross data packets combined to the available bandwidth estimation performed by RCT allows this protocol to have better performance than ABv6 and OSPFv6.

When the network becomes denser (between 20 and 40 flows), φ decreases, which is expected as the available bandwidth per link decreases and lower quality routes are established. However, RCT can also transmit about 60% of QoS flows.

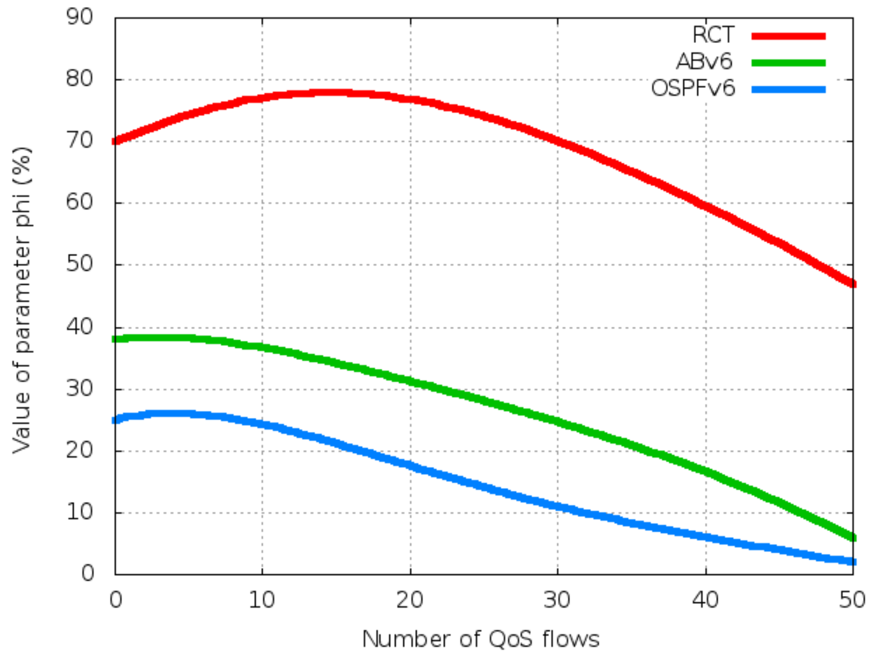

Figure 4. Acceptance rate of flows with RCT, ABv6 and OSPFv6

Finally, when the network becomes very dense (between 40 and 50 flows), the residual bandwidth becomes low and even a reduction of throughput of cross traffic cannot release enough available bandwidth to allow QoS flows to be transmitted with their throughput requirements. Nevertheless, RCT still correctly transmits about 48% of QoS flows while all the others protocols transmit in the best case almost than 11%.

Protocols	Total Aggregated data for cross traffic in MB
OSPFv6	8794
ABv6	5290
RCT	2348

Table 1. Total aggregated data of cross traffic for RCT, ABv6 and OSPFv6

Table 1 presents the total amount of cross traffic aggregated through the network. As it can be expected, RCT provides the lower value because of the reduction scheme of cross traffic throughput in order to increase QoS flows acceptance rate. This reduction for RCT is respectively about 55% and 73% comparatively to ABv6 and OSPFv6.

6 Conclusion and future works

In this paper, we have presented RCT, a protocol which guarantees bandwidth of QoS flows by adapting effectively and dynamically the throughputs of cross transmissions when it is necessary. Our protocol relies on an estimation of the available bandwidth differentiated according to the type of packets (QoS or cross data packets). With these features, RCT increases the acceptance ratio of QoS flows, while providing a better usage of the radio medium. Furthermore, the effectiveness of our protocol is shown through simulations, where RCT effectively manages the throughputs of QoS transmissions by dynamically adapting rate of close cross traffic, compared to other protocols like

ABv6, and OSPFv6.

As future works, we plan to carry out more complete and exhaustive simulation models in more diverse topologies and compare it with other available bandwidth technique in order to refine the available bandwidth measurement.

References

[1]. Rob Coltun, Dennis Ferguson, John Moy, and A Lindem. *Ospf for ipv6*. IETF RFC2740, 2:839–841, 2008.

[2]. Marshall Crocker, GY Lazarou, Julie Baca, and Joe Picone. *A bandwidth determination method for ipv6-based networks*. International Journal of Computers & Applications, 31(2), 2009.

[3]. Priyanka Dhiman and Arvind Kalia. *Available bandwidth measurement of campus wide optical fiber network using packet pair technique*. International Journal of Computer Applications, 65(9), 2013

[4]. Christian Huitema. *IPv6: the new Internet protocol*, Volume 2. Prentice Hall Englewood Cliffs, New Jersey, 1996.

[5]. Mahamat Hassan Borgou, Cheikh Sarr. *Estimating available bandwidth in wired IPv6 networks*. International Journal of Computer Communication and Collaboration (CCC), Volume 2, Numéro 4, pages 28 - 38, November 2014

[6]. Peter Loshin. *IPv6: Theory, protocol, and practice*. Morgan Kaufmann, 2004.

[7]. Liu Min, Li Zhongcheng, Shi Jinglin, and Guo Xiaobing. *Estimating available bandwidth in ipv6 networks*. In Communications of APCC 2003. The 9th Asia-Pacific Conference, volume 3, pages 939–944. IEEE, 2003.

[8]. Gopalaswamy Soora and Vernon Lawton Tice. *Multimedia distribution network including video switch*, May 26 1998. US Patent 5,756,280.

[9]. Li Xing-feng, Wang Yi-zhi, and Luo Wan-ming. *A novel ipv6 networks measuring algorithm for locating available bandwidth bottleneck*. In Advanced Communication Technology, the 9th International Conference, volume 2, pages 1195–1200. IEEE, 2007.

[10]. Zhang, Lixia, DEERING, Steve, ESTRIN, Deborah, et al. RSVP: A new resource reservation protocol. Network, IEEE, 1993, vol. 7, no 5, p. 8-18.

[11]. Juan Zhou, Yi Wang, and Gang Hu. End-to-end performance measurement model on diffserv domain in ipv6 network. In Networked Computing and Advanced Information Management (NCM), 2010 Sixth International Conference on, pages 203–206. IEEE, 2010.