An Adaptive Fuzzy Type-2 Control Double Token Leaky Bucket and Back-pressure over High-Speed Network

Somchai Lekcharoen
Faculty of Information Technology, Rangsit University, Thailand
Email:s_lekcharoen@yahoo.com

***Abstract*—High-speed communication network describes about high bandwidth and low delay communication. The problem in delay occurs traffic congestion. A method to solve this problem, we use a policing mechanism scheme. It is a method help monitor the amount of ingress traffic. If congestion occurs at the buffer before entering the network. Another approach must drop incoming frames from which buffer is not available and has to rely on the end-to-end protocols for the recovery of lost frames. In this way, it may not be able to cope their quality-of-service (QoS) requirements because it must have more delay time. However, one way to solve this problem, we use Fuzzy type-2 control double token leaky bucket and back-pressure to control network congestion but it is suitable for low traffic. It could help to improve the performance in policing mechanisms much better than conventional policing one while various types of burst/silence traffic are being generated.**

***Index Terms*—type-2fuzzy control, policing mechanism**

I. Introduction

In high speed networks, the traffic sources always become activated at the reaching peak rate. Network congestion have occurred this point. To prevent this condition, policing mechanisms were introduced. It can degrade the main performance measures such as dropped frame, bandwidth allocation, frame delay, throughput and other grade of service measures. There have been a lot of previous studies involving traffic policing mechanisms [1], [2], [3], [4].

Currently, the policing mechanism scheme is wildly used to control network congestion. The previous papers have been proposed involving traffic policing mechanism schemes. But they are difficult to obtain the proper and understandable modeling representations. This difficulty has simulated the development of alternative modeling and control techniques which include fuzzy logic based ones. Type-2 Fuzzy control may show the way to the models that express the behavior of systems suitably for their application in fuzzy control. Thus due to the requirement for low-cost but reliable models, the type-2 fuzzy modeling approach may be a useful complement to traditional modeling. The type-2 fuzzy control approach is suitable for both the complexity and uncertainty during the increase of the system. This is of great practical significance, since modeling is usually the bottleneck for the application of effective control.

There are a number of previous studies involving fuzzy control traffic policing mechanism schemes. In this paper, we have proposed a model for Fuzzy type-2 control double token leaky bucket and back-pressure over high-speed network which it is not mention.

This paper is organized as follows. In Section II, we propose policing mechanisms, backpressure in literature. Section III, we define the model of a type-2 fuzzy control policing mechanism scheme. Section IV, we define the simulation model. Section V, we describe the results and analysis. Section VI some conclusion and recommendation for future research are drawn.

II. Description and Modeling of Traffic Policing

Traffic policing mechanism schemes allow us to control the maximum rate of traffic sent or received on an interface during the entire active phase and must operate in real time. These mechanisms have been proposed and are described in the following sections.

In addition to these requirements, mechanism of parameter violations must be short to avoid flooding of the relatively small buffers in the network. To eliminate these conflicting requirements, several policing mechanisms have been proposed [1], [2] as described in the following sections.

A. Traffic Source Models

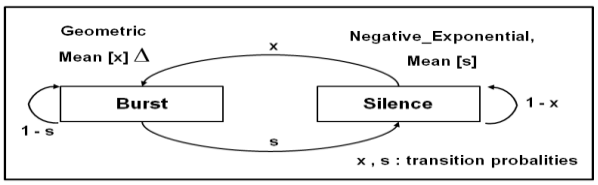

Figure. 1. The burst/silence traffic model.

In this section, we describe the traffic model used in the simulation. In our simulation, a burst traffic stream from a single source is modeled as burst/silence traffic stream. The burst/silence ratio is strictly alternating. The number of packets per burst is assumed to have a geometric distribution with mean E[X]; the duration of the silence phases is assumed to be distributed according to a negative-exponential distribution with mean E[S]; and inter-packet arrival time during a burst is given by Δ. With

Manuscript received July 1, 2012; revised September 10, 2012.

doi: 10.12720/lnit.1.1.48-52

$$\textit{mean burst duration} = E[X]\,\Delta \quad (1)$$
$$\textit{mean silence duration} = E[S] \quad (2)$$
$$\textit{mean cycle duration} = E[X]\,\Delta + E[S] \quad (3)$$

B. Policing Mechanism Models

The policing mechanism schemes are done at the edges of the network for frame-based traffic. This mechanism decides whether to accept a unit of incoming frames or drop frames. Nevertheless, this study selected the Token Leaky Bucket (LB) only.

C. Token Leaky Bucket Process Model

This study selected the Token leaky bucket (LB) only.

The Token leaky bucket has two buckets, one for storing incoming frames in a queue with a capacity of K bits, another one for storing a maximum of β so-called token. Each coming bit needs to take out a token from the token bucket to be forwarded, and the token bucket is filled with a rate of ρ tokens per time unit. If the token bucket is full, no more tokens can be added to the token bucket. If the traffic queue is full, incoming frames are dropped. However, the committed sustainable bit rate is limited by ρ [5],[6].

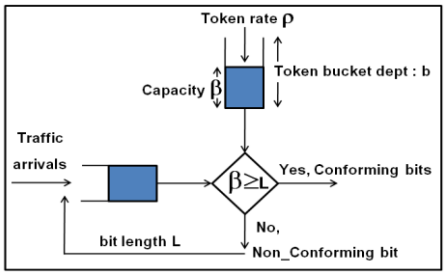

Figure 2. Token leaky bucket mechanism.

Double Token Leaky Bucket Process Model

The Traffic shaping can be used a double token leaky bucket algorithm that requires a high speed network. As indicated by the name, the behavior of a Token leaky bucket is similar to a bucket with a hole in its bottom. If data flows into the queue faster than token, then the queue over flows. This causes data to be dropped until there is enough room in the queue to accept new data. The token leaky bucket is described in Figure 2. A double token leaky bucket as a traffic monitor is shown in Figure 3. If the first token leaky bucket is filled up frames until over flow, dropped frames go to the second token leaky bucket.

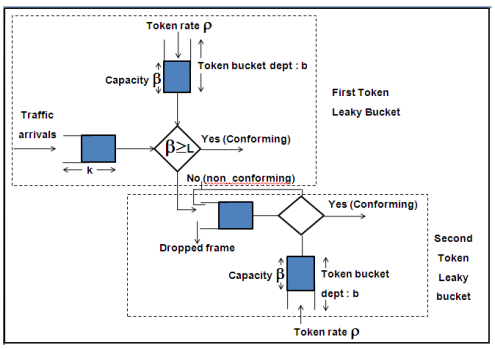

Figure. 3. Double token leaky bucket model

D. Backpressure Algorithm

The backpressure algorithm works like XON/XOFF techniques with a purpose to avoid buffer overflows and temporary network congestion. The XOFF flow control message is sent to source when buffer of destination is filled up frame until overflow. When the Source receives a XOFF message, it stops sending frames until it receives a XON message from the same destination. The XON message is triggered when the buffer of destination has decreased below the lower threshold.

In the backpressure algorithms, when frames arrives at destination' buffer, the backpressure algorithm is activated. If destination' buffer is below the threshold, it sends message to the source. The source can increase a half the transmission rate. If destination' buffer reaches the upper threshold, then destination sends a message to source to reduce a half the transmission rate. The backpressure is suitable for a connection-oriented network that allows hop-by-hop flow control. The backpressure algorithm is showed with the pseudo code as follows.

// The goal of backpressure algorithm wants to control the //traffic rate. If the buffer is filled up frames until reaching //threshold then the destination hop sends the message to the //source and it reduces to half transmission rate.

Start Check:

IF buffer of destination exceeds the upper threshold

THEN GOTO Stop:

ELSE {

IF $Q_{DESTN} >= Q_{THRESHOLD}$

THEN Destination sends feedback to source and source reduces traffic rate to half.

GOTO Start Check:

ELSE Destination sends feedback to source and source increases traffic rate to half.

GOTO Start Check:

} Stop:

III. Type-2 Fuzzy Control Prior Buffer

In this section, we initially first describe the concept of type-2 fuzzy and type-2 fuzzy control prior buffer in policer which meets the requirements of performance implementation of high speed networks.

A. Basic Concepts of Type-2 Fuzzy Set [7], [8], [9].

The type-2 fuzzy set appears to be handled more uncertainly than fuzzy set. A type-2 fuzzy set incorporates uncertainly with the membership function into the fuzzy set theory. If there is no uncertainty, then a type-2 fuzzy set will reduces to a type-1 fuzzy set. In

order to distinguish between a type-1 fuzzy set and a type-2 fuzzy set, A denotes a type-1 fuzzy set, whereas Ã denotes the comparable type-2 fuzzy set. The feature of Ã versus A is the membership function values. They have a continuous range of values between 0 and 1.

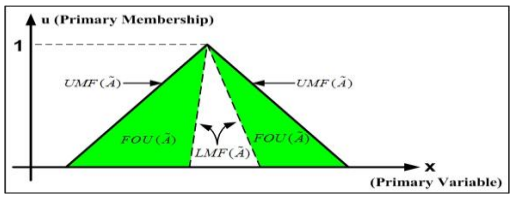

Figure. 4. FOU for an interval type-2 fuzzy set. Many other shapes are also possible for the FOU.

The FOU is described by its two bounding functions (Fig. 3), a lower membership function (LMF) and an upper membership function (UMF), both of which are type-1 fuzzy sets. We can use type-1 fuzzy set mathematics to characterize and work with interval type-2 fuzzy sets. It can be said that Type-2 Fuzzy Sets are suitable for *rule-based fuzzy logic systems* (FLSs) because they can handle uncertainties whereas Type-1 fuzzy cannot handle uncertainties. A diagram of a type-2 FLS is depicted in Fig. 4.

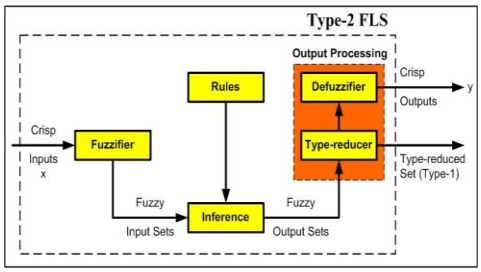

Figure. 5. Type-2 Fuzzy logic systems.

Fuzzy sets are associated with the terms of IF THEN ELSE rules, and with the inputs to and the outputs of the Fuzzy set. Membership functions are used to describe these fuzzy sets. The Type-2 Fuzzy sets have an interval membership functions.

In output processing of a type-1 Fuzzy Sets which is called *Defuzzification* maps a type-1 fuzzy set into a number. Nevertheless, it is more complicated for an interval type-2 Fuzzy Set because it is going from an interval type-2 fuzzy set to a number which (usually) requires two steps (Fig. 5). The first step, called *type-reduction* is where an interval type-2 fuzzy set is reduced to an interval-valued type-1 fuzzy set. There are as many type-reduction methods as there are in type-1 defuzzification methods. The second step of Output Processing, which occurs after type-reduction, is still called *defuzzification*. Since a type-reduced set of an interval type-2 fuzzy set is always a finite interval of numbers, the defuzzified value is just the average of the two end-points of this interval.

B. Regulator Input Fuzzification

Input variables are transformed into fuzzy set (fuzzification) and manipulated by a collection of IF-THEN fuzzy rules, assembled in what is known as the fuzzy inference engine, as shown in the Fig. 5.

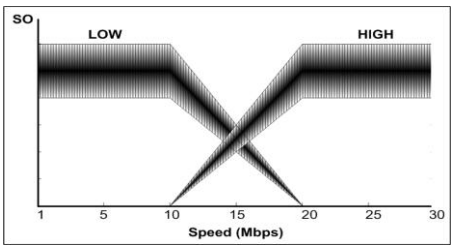

Figure. 6. Membership function of SO input variable.

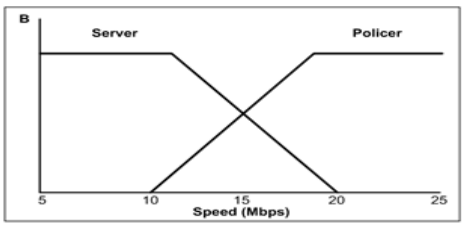

Figure. 7. Membership function of B output variable.

C. Inference, Fuzzy Rules and Defuzzification

Fuzzy sets are involved only in rule premises. Rules consequences are crisp functions of the output variables. There is no separate defuzzification step. Based on our defined measurement of input variables and their membership functions, the fuzzy system can be described by five fuzzy IF-THEN rules, each of which locally represents a linear input-output relation for the regulator. In Fig. 8, it shows simple fuzzy rules used in the experiment.

IF So is Low (L) AND various types of burst/silence is narrow THEN go to server
IF So is Low (L) AND various types of burst/silence is wide THEN go to PLC
IF So is High (H) THEN go to PLC

Figure. 8. The fuzzy rules.

Fig. 6, Fig. 7 and Fig. 8 respectively show the membership functions of the linguistic values of the input variables So and also the output variables B being taken. Analysis of the fuzzy system rules (Fig. 8) shows that sources are Low (L) and various types of burst/silence is narrow THEN they go to server. If sources are Low (L) and various types of burst/silence is wide THEN they go to PLC (Policing Mechanism). If sources are High (H) THEN they go to PLC.

In our models, Type-2 Fuzzy Control (T2F) uses a set of rules (Fig. 6, Fig. 7 and Fig. 8). The selection of basic rules is based on our experience and beliefs on how the system should carry out. Input traffics allow a burst traffic stream (burst/silence stream) to fluctuate the network controlled by fuzzy controller.

IV. Simulation Model

The following Fig. 9 shows a simulation model used in this paper.

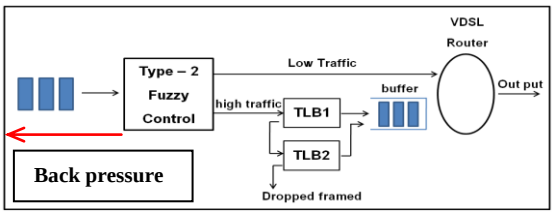

Figure. 9. Simulation model.

A. Input traffic

This research confines the discussion mainly on data. Data sources are generally bursty in nature whereas voice and video sources can be continuous or bursty, depending on the compression and coding techniques used [6].

B. Characteristics of Queuing Network Model

There are three components with certain characteristics that must be examined before the simulation models are developed.

Arrival Characteristics

The pattern of arrival input traffic mostly is characterized to be *Poisson Arrival Processes.* Like several random events, Poisson arrivals occur such a manner that for each increment of time (*T*), no matter how large or small, the probability of arrival is independent of any previous history. These events may be individual labels, a burst of labels, label or packet service completions, or other arbitrary events. The probability of the inter-arrival time between event t, is defined by the inter-arrival time probability density function (pdf). The following formulae give the resulting probability density function (pdf), which theinter-arrival time t is larger than some value x when the average arrival rate is λ events per second:

$$F_x(t) = P(X \le t) = \int_0^t e^{-\lambda x} dx \tag{4}$$

$$f_x(t) = \begin{cases} e^{-\lambda t}, & for\ t \ge 0 \\ 0, & for\ t < 0 \end{cases} \tag{5}$$

In this paper, we adopt the ON/OFF burst/silence model.

Service facility characteristics

In this paper, service times are randomly distributed by the *exponential probability distribution*. This is a mathematically convenient assumption if arrival rates are Poisson distributed. In order to examine the traffic congestion at output of VDSL (Very High Speed Digital Subscriber Line) downstream link (15Mbps) [6], the service time in the simulation model is specified by the speed of output link, giving that a service time is 216 μs per frame where the frame size is 405 bytes [6].

V. Results and Analysis

The comparison among leaky bucket(LB), type-1 fuzzy(T1F) and Type-2 fuzzy control double token leaky bucket and backpressure(TDBT2F) are shown in Fig. 10-12.

This section indicates simulation results from leaky bucket,Type1 fuzzy and Type-2 fuzzy control double token leaky bucket and backpressure performance will be compared. The input frames (frame rate varies from 5 Mbps to 20 Mbps) with various types of burst/silence performed simulation results are shown in Fig. 10. It clearly determines that the TDBT2F is the best of throughput guarantee. Throughput is one of factor of QoS to help guarantee higher reliability of network performance. In conclusion, the TDBT2F may assure higher reliability to handle uncertain traffics compared to the other type-1 fuzzy (T1F) and leaky bucket (LB).

Fig. 11 show the results in the sense that TDBT2F will produce lowest dropped frames compared to the other schemes. In other words, we can help conserve the conforming frames by reducing number of dropped frames. A regular network may cause a poor QoS by higher non-conforming or dropped frames.

In Fig. 12, the result determines that the utilization of the LB scheme is the lowest. From this viewpoint, the processing unit will be available for other sources in terms of sharing. The result is in the line of low processing power required by LB because LB is likely to produce fewer conforming frames and higher dropped frames. Most frames are discarded before transferring (entering the network) to the entrance of the network. It seems like LB makes less congestion but it will reflect the lower throughput in return. Both T1F and TDBT2F result higher in utilization factor, but the figure does not go beyond the saturated point (as high as 59%). It is because both schemes make more conforming frames as well as higher number in successful retries.

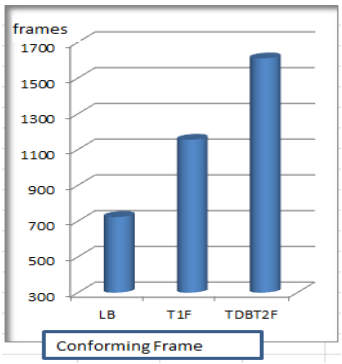

Figure. 10. Illustrates conforming frames comparison among leaky bucket (LB), Type-1 Fuzzy (T1F), and Type-2 Fuzzy (TDBT2F).

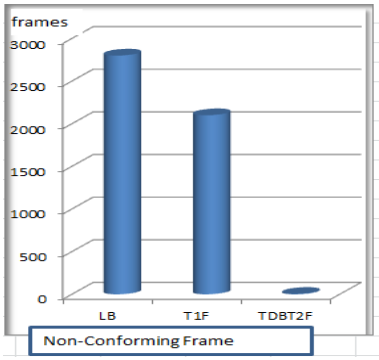

Figure 11. Ilustrates non-conforming frames comparison among leaky bucket (LB), Type-1 Fuzzy (T1F), and Type-2 Fuzzy (TDBT2F).

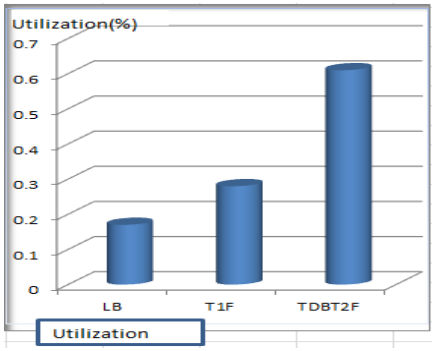

Figure 12. Illustrates the utilization comparison among leaky bucket (LB), Type-1 Fuzzy (T1F), and Type-2 Fuzzy (TDBT2F).

VI. Conclusions and Recommendations for Future Research

In this paper, we carried out a comprehensive study to investigate the performance of three selected traditional policing mechanism schemes, type-1 fuzzy control and TDBT2F with various types of burst/silence traffic. The study was accomplished through simulation after developing an analytical queuing model.

We found that based on simulation results in general, the TDBT2F appeared to be the best outperforming compared to the others (type-1 fuzzy control and traditional policing mechanism scheme) in terms of maximizing the number of conforming frames; less non-conforming frame. It is also believed that TDBT2F seem to be suitable for data and multimedia under various types of burst/silence traffic condition.

References

[1] A. AlWehaibi, A. Agarwal, S. AlWakeel, N. E. Rikli, and A. ElHakeem, "Performance behavior evaluation of Internet congestion control policing mechanisms," *IEEE CCECE*, vol. 2, pp. 1017-1020, May 2003.

[2] [T. Gouda, et al., "Application of policing mechanisms for broadband networks: issues and difficulties," *AINA 2005*, vol. 1, pp. 183-188, March 2005.

[3] A. Niruntasukrat and W. Benjapolakul, "A novel scheme for policing mechanism in ATM networks: feedback fuzzy leaky bucket," *IEEE International Symposium on Circuits and Systems*, vol. 2, pp. 161-164, May 2001.

[4] K. Dimyati and Y. T. Chin, "Policing mechanism and cell loss priority control on voice cells in ATM networks using fuzzy logic," *IEE Proceedings Communications*, vol.147, no. 4, pp. 239-244, August 2000.

[5] W. Cheng-Shong, H. Ming-Hsien, and C. Kim-Joan, "Traffic shaping for TCP networks: TCP leaky bucket," in *Proc. IEEE Region 10 Conference on Computers, Communications, Control and Power Engineering*, vol. 2, pp. 809-812, October 2002.

[6] S. Lekcharoen, et. al., "Performance Evaluation of VDSL Network with Fuzzy Control Policing Mechanisms," in *Proc. International Conference on Telecommunications and Computer Networks*, pp. 56-60, 2004.

[7] Q. Liang, N. N. Karnik, and J. M. Mendel, "Connection admission control in ATM networks using survey-based type-2 fuzzy logic systems," *IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews*, vol. 30, pp. 329-339, August 2000.

[8] L. Li, W. H. Lin, and H. Liu, "Type-2 fuzzy logic approach for short-term traffic forecasting," *IEE Proceedings*, vol. 153, no. 1, pp. 33-40, March 2006.

[9] E. Jammeh, M. Fleury, C. Wagner, H. Hagras, and M. Ghanbari, "Interval type-2 fuzzy logic congestion control of video streaming," *IET 4th International Conference on Intelligent Environments*, pp. 1-8, July 2008.

Somchai Lekcharoen was born in Bangkok, Thailand in 1965.He received the M.Sc. degree in Information Technology from King Mongkut's University of Technology in 1998, Thonburi Campus, Thailand. He received his Ph.D. in Computer Science at Assumption University of Thailand in 2008.

He is an assistant professor of faculty of Information technology, Rangsit University, Thailand. He has published more that 30 scientific papers. He is scientific research and for leadership in the area of science in Telecommunication engineering and his research interest is today focused on congestion control, fuzzy logic and network of queue.