ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 9, September 2014

With Blurry Judgment Organize To Present Intellectual Travel Management Service for High-Speed Networks

A.Laxman, S.Arvind

Student, Dept of Computer Science & Engineering, CMR Institute of Technology, Hyderabad, India

HOD, Professor, Dept of Computer Science & Engineering, CMR Institute of Technology, Hyderabad, India

ABSTRACT: We deal with this open issue by proposing a fully distributed cooperative solution that is robust against self-regulating and colluding adversaries, and can be impair only by an overwhelming presence of adversaries. Results show that our protocol can thwart more than 99 percent of the attacks under the best possible environment for the adversaries, with minimal false positive rates. In view of the fast-growing Internet traffic, this paper propose a distributed traffic management framework, in which routers are deployed with intelligent data rate controllers to tackle the traffic mass. Unlike other explicit traffic control protocols that have to estimate network parameters (e.g., link latency, bottleneck bandwidth, packet loss rate, or the number of flows) in order to compute the allowed source sending rate, our fuzzy-logic-based controller can measure the router queue size directly; hence it avoids various potential performance problems arising from parameter estimations while reducing much utilization of computation and memory resources in routers. As a network parameter, the queue size can be truthfully monitored and used to proactively decide if action should be taken to regulate the source sending rate, thus increasing the resilience of the network to traffic congestion. The communication QoS (Quality of Service) is assured by the good performances of our scheme such as max-min fairness, low queuing delay and good robustness to network dynamics**.**

KEYWORDS: Congestion Control, Fuzzy Logic, Neighbour Position Verification

I. INTRODUCTION

We focus on the latter aspect, here in after referred to as neighbor position verification (NPV for short). Specifically, we deal with a mobile ad hoc network, where a pervasive infrastructure is not present, and the location data must be obtained through node-to-node communication. Such a scenario is of particular interest since it leaves the door open for adversarial nodes to misuse or disrupt the location-based services. For example, by advertising forged positions, adversaries could bias geographic routing or data gathering processes, attracting network traffic and then eavesdropping or discarding it. Similarly, counterfeit positions could grant adversaries unauthorized access to location-dependent services, let vehicles forfeit road tolls, disrupt vehicular traffic or endanger passengers and drivers.
In this context, the challenge is to perform, in absence of trusted nodes, a fully distributed, lightweight NPV procedure that enables each node to acquire the locations advertised by its neighbors, and assess their truthfulness. We therefore propose an NPV protocol that has the following features:
. It is designed for spontaneous ad hoc environments, and, as such, it does not rely on the presence of a trusted infrastructure or of a priori trustworthy nodes;
. It leverages cooperation but allows a node to perform all verification procedures autonomously. This approach has no need for lengthy interactions,
e.g., to reach a consensus among multiple nodes, making our scheme suitable for both low- and highmobility environments;
. It is reactive, meaning that it can be executed by any node, at any point in time, without prior knowledge of the neighborhood;
. It is robust against independent and colluding adversaries;

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 9, September 2014

. It is lightweight, as it generates low overhead traffic. Additionally, our NPV scheme is compatible with state-of- the-art security architectures, including the ones that have been proposed for vehicular networks which represent a likely deployment environment for NPV. Our new scheme pays attention to the following methodologies as well as the merits of the existing protocols. Firstly, in order to keep the implementation simple, like TCP, the new controller treats the network as a black box in the sense that queue size is the only parameter it relies on to adjust the source sending rate. The adoption of queue size as the unique congestion signal is inspired by the design experience of some previous AQM controllers (e.g., RED and API-RCP) in that queue size can be accurately measured and is able to effectively signal the onset of network congestion. Secondly, the controller retains the merits of the existing rate controllers such as XCP and RCP by providing explicit multi-bit congestion information without having to keep per-flow state information. Thirdly, we rely on the fuzzy logic theory to design our controller to form a traffic management procedure. Finally, we will employ OPNET modeler to verify the effectiveness and superiority of our scheme. The contributions of our work lie in: 1) using fuzzy logic theory to design an explicit rate-based traffic management scheme for the high-speed IP networks; 2) the application of such a fuzzy logic controller using less performance parameters while providing better performances than the existing explicit traffic control protocols; 3) The design of a Fuzzy Smoother mechanism that can generate relatively smooth flow throughput; 4) the capability of our algorithm to provide max-min fairness even under large network dynamics that usually render many existing controllers unstable.

II. COOPERATIVE NPV: AN OVERVIEW

We propose a fully distributed cooperative scheme for NPV, which enables a node, hereinafter called the verifier, to discover and verify the position of its communication neighbors. For clarity, here we summarize the principles of the protocol as well as the gist of its resilience analysis. Detailed discussions of message format, verification tests, and protocol resilience are provided in a verifier, S, can initiate the protocol at any time instant, by triggering the 4-step message exchange depicted in its 1-hop neighborhood. The aim of the message exchange is to let S collect information it can use to compute distances between any pair of its communication neighbors. To that end, POLL and REPLY messages are first broadcasted by S and its neighbors, respectively. These messages are anonymous and take advantage of the broadcast nature of the wireless medium, allowing nodes to record reciprocal timing information without disclosing their identities. Then, after a REVEAL broadcast by the verifier, nodes disclose to S, through secure and authenticated REPORT messages, their identities as well as the anonymous timing in order they collected. The verifier S uses such data to match timings and identities; then, it uses the timings to perform ToF-based ranging and compute distances between all pairs of communicating nodes in its neighborhood.

Once S has derived such distances, it runs several position verification tests in order to classify each candidate neighbor as either:

1. Verified, i.e., a node the verifier deems to be at the claimed position;
2. Faulty, i.e., a node the verifier deems to have announced an incorrect position;
3. Unverifiable, i.e., a node the verifier cannot prove to be either correct or faulty, due to insufficient information.

Clearly, the verification tests aim at avoiding false negatives (i.e., adversaries announcing fake positions that are deemed verified) and false positives (i.e., correct nodes whose positions are deemed faulty), as well as at minimizing the number of unverifiable nodes. We remark that our NPV scheme does not target the creation of a consistent "map" of neighborhood relations throughout an ephemeral network: rather, it allows the verifier to independently classify its neighbours.

III. NPV PROTOCOL

We detail the message exchange between the verifier and its communication neighbors, followed by a description of the tests run by the verifier.

Protocol Message Exchange POLL message. The verifier starts the protocol by broadcasting a POLL whose transmission time t_S it stores locally .The POLL is anonymous, it does not carry the identity of the verifier, 2) it is transmitted employing a fresh, software-generated MAC address, and 3) it contains a public key K_S^i taken from S's pool of anonymous one-time use keys that do not allow neighbors to map the key onto a specific node. We stress that indict the identity of the verifier hidden is important in order to make our NPV healthy to attacks. Since a source address has to be included in the MAC-layer header of the message, a fresh, software-generated MAC address is

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 9, September 2014

needed; note that this is considered a part of emerging cooperative systems. Counting a one-time key in the POLL also ensures that the message is fresh (i.e., the key acts as a nonce).

REPLY message.: A communication neighbor that receives the POLL stores its response time t and extracts a random wait interval has elapsed, X broadcasts an anonymous REPLY message using a fresh MAC address, and locally records its broadcast time t For implementation feasibility, the physical layer transmission time cannot be embossed on the REPLY, but it is stored by X for later use. The REPLY contains some information encrypted with S public key, specifically The POLL reaction time and a nonce REPLY to the next message sent by X: we refer to these data as X's commitment, The hash h derived from the public key of the verifier, K, is also included to bind POLL and REPLY belonging to the same message exchange.

REVEAL message: After a time the verifier broadcasts a REVEAL message using its real MAC address (Algorithm accounts for the propagation and contention lag of REPLY messages scheduled at time T max
, and T is a casual time added to thwart jamming efforts on this message. The REVEAL contains: 1) a map, that associates each commitment C received by the verifier to a temporary identifier a proof that S is the author of the original POLL through the encrypted has the verifier identity, i.e., its
certified public key and signature Note that using certified keys curtails continuous attempts at running the protocol by an adversary who aims at learning neighbor positions (i.e., at becoming knowledgeable)
or at launching a jam attack .

REPORT message: Once the REPORT message is broadcast and the identity of the verifier is known, each neighbor X that previously received S's POLL unicasts to S an encrypted, signed REPORT message. The REPORT carries X's position, the transmission time of X's
REPLY, and the list of pairs of reception times and provisional identifiers referring to the REPLY broadcasts X received The identifiers are obtained from the map included in the REVEAL message. Also, X discloses its own identity by including in the message its digital name and certified public key; through the nonce, it correlates The REPORT to its previously issued REPLY. We remark that all sensitive data are encrypted using S s public key, so that eavesdropping on the wireless channel is not possible. At the end of the message exchange, only the verifier knows all positions and timing information. If needed, certified keys in REPORT messages allow the matching of such data and node identities.

Position Verification: Once the message exchange is concluded, S can decrypt the usual data and acquire the position of all neighbors that participate in the protocol,

The Direct Symmetry Test (DST):DST is the first verification performed by S and is detailed in There, denotes the absolute value operator the euclidean distance between locations .In the DST, S verifies the direct links with its communication neighbors. To this end, it checks whether reciprocal ToF-derived distances are consistent1) with each other, 2) with the position advertised by the neighbor, and 3) with a proximity range R. The latter corresponds to the maximum nominal transmission range, and upper bounds the distance at which two nodes can communicate. More specifically, the first check verifies that the distances, obtained from ranging, do not differ by more than twice the ranging error plus a tolerance value accounting for node spatial movements during the protocol execution. The second check verifies that the position advertised by the neighbor is consistent with such distances, within an error margin of although trivial, this check is fundamental since it correlates positions to computed distances: without it, an attacker could fool the verifier by simply advertising an arbitrary position along with correct broadcast transmission and reception timings.

The Cross-Symmetry Test (CST): In implements cross verifications, i.e., it checks on the information mutually gathered by each pair of communication neighbors. The CST ignores nodes already declared as faulty by the DST and only considers nodes that proved to be communication neighbors between each other, i.e., for which derived mutual distances are available However, pairs of neighbors declaring collinear positions with respect to S are not taken into account is the line passing by points. As shown in the next section, this choice makes our NPV robust to attacks in particular situations. For all other pairs the CST verifies the symmetry of the reciprocal distances their consistency with the positions declared by the nodes and with the proximity range For each neighbor X, S maintains a link counter l and a mismatch counter

The Multilateration Test (MLT)

MLT, in Algorithm 5, ignores nodes already tagged as faulty or unverifiable and looks for suspect neighbors in. For each neighbor X that did not notify about a link reported by another node is computed and added to the

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

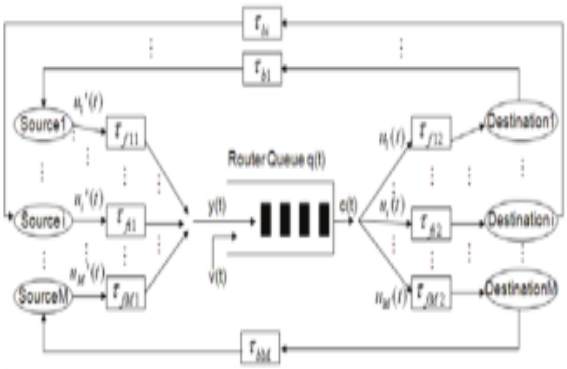
(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 9, September 2014

Such a curve is the locus of points that can generate a transmission whose Time Difference of Arrival (TDoA) at S and Y matches that measured by the two nodes, i.e It is easy to verify that such a curve is a hyperbola temporary through the actual position of X.

IV. TRAFFIC MANAGEMENT PRINCIPLE AND MODELING

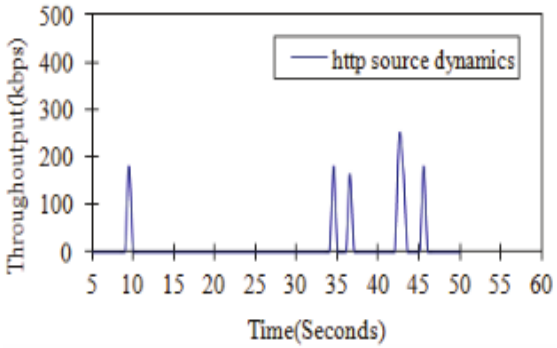
We consider a backbone network interconnected by a number of geographically distributed routers, in which hosts are attached to the access routers which cooperate with the core routers to enable end-to-end communications. Congestion occurs when many flows traverse a router and because its IQSize (Instantaneous Queue Size) to exceed the buffer capacity, thus making it a bottleneck in the Internet. Since any router may become bottleneck along an end-to-end data path, we would like each router to be able to manage its traffic. Below is the general operation principle of our new traffic management/control algorithm. Inside each router, our distributed traffic controller acts as a data rate regulator by measuring and monitoring the IQSize. As per its application, every host (source) requests a sending rate it desires by depositing a value into a dedicated field *Req_rate* inside the packet header. This field can be updated by any router en route. Specifically, each router along the data path will compute an allowed source transmission rate according to the IQSize and then compare it with the rate already recorded in *Req_rate* field. If the former is smaller than the latter, the *Req_rate* field in the packet header will be updated; otherwise it remains unchanged. After the packet arrives at the destination, the value of the *Req_rate* field reflects the allowed data rate from the most congested router along the path if the value is not more than the desired rate of the source. The receiver then sends this value back to the source via an ACK (ACKnowledgment) packet, and the source would update its current sending rate accordingly. If no router modifies *Req_rate* field, it means that all routers en route allow the source to send its data with the requested desired rate.



System model of an AQM router.

PERFORMANCE EVALUATION

The capability of the IntelRate controller is demonstrated by performance evaluations through a series of experiments.



Http sessions example.

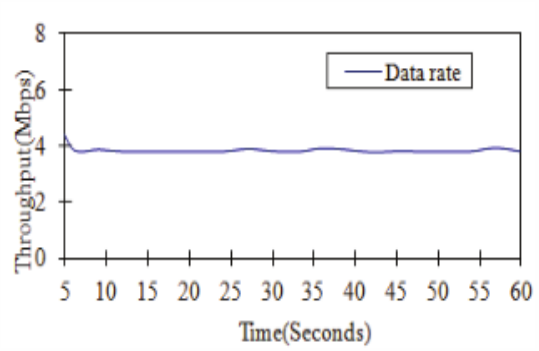
ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 9, September 2014

In order to demonstrate and discuss the robustness of our IntelRate controller, our experiments would focus on the testing of the 100 long-lived ftp flows, unless otherwise stated. The 100 sporadic short-lived http flows just act as the disturbance to the ftp traffic and their transfer size follows the real web traffic scenario; it has a Pareto distribution with a mean transfer size of 30 packets. The arrivals of http flows follow a think-time [50] uniformly distributed in [0.1s, 30s]. One of the http session examples is shown in Fig.



The experiments were conducted using OPNET Modeler 11.5 [51] on an Intel Core TM2 Quad platform with 2.40GHz processor. Typical simulated time is set according to the specific experiment scenario. The simulation time depends on bottleneck bandwidth and the simulated time. A typical simulation run usually takes hours or days. For example, in order to observe the source throughput behavior before and after the network parameter change, we set a longer simulated time for such an experiment than max-min fairness experiment. The number of packets generated in an experiment is related to the TBO value, the bandwidth, the simulated time and the traffic intensity. The controller is evaluated by the following performance measures.

1) Source throughput (or source sending rate) is defined to be the average number of bits successfully sent out by a source per second, i.e. bits/second [51]. Here, a bit is considered to be successfully sent out if it is part of a packet that has been successfully sent.

2) IQSize is the length of the bottleneck buffer queue (measured in packets) seen by a departing packet.

3) Queueing delay is the waiting time of a packet in the router queue before its service. Measurements are taken from the time the first bit of a packet is received at the queue until the time the first bit of the packet is transmitted.

4) Queueingjitter is the variation of queueing delay due to the queue length dynamics, and is defined as the variance of the queuing delay.

5) Link (or bottleneck) utilization is the ratio between the current actual throughput in the bottleneck and the maximum data rate of the bottleneck. It is expressed as a fraction less than one or as a percentage.

6) Packet loss rate is the ratio between the number of packet dropped and the number of total packets received per second by the bottleneck.

7) Max-min fairness: A feasible allocation of rates is 'maxmin fair' if and only if an increase of any rate within the domain of feasible allocations must be at the cost of a decrease of some already smaller or equal rates. Since the behavior and performance of the sources within each group are quite similar, in the following experiments we shall only show the results of one source from each ftp group or http group for brevity reason.

V. CONCLUSION

A novel traffic management scheme, called the IntelRate controller, has been proposed to manage the Internet congestion in order to assure the quality of service for different service applications. The controller is designed by paying attention to the disadvantages as well as the advantages of the existing congestion control protocols. As a distributed operation in networks, the IntelRate controller uses the instantaneous queue size alone to effectively throttle the source sending rate with max-min fairness. Unlike the existing explicit traffic control protocols that potentially suffer from performance problems or high router resource consumption due to the estimation of the network parameters, the IntelRate controller can overcome those fundamental deficiencies. To verify the effectiveness and superiority of the IntelRate controller, extensive experiments have been conducted in OPNET modeler. In addition to

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 9, September 2014

the feature of the FLC being able to intelligently tackle the nonlinearity of the traffic control systems, the success of the IntelRate controller is also attributed to the careful design of the fuzzy logic elements.

REFERENCES

[1] M. Welzl, *Network Congestion Control: Managing Internet Traffic*. John Wiley & Sons Ltd., 2005.
[2] R. Jain, "Congestion control and traffic management in ATM networks:recent advances and a survey," *Computer Networks ISDN Syst.*, vol. 28,no. 13, pp. 1723–1738, Oct. 1996.
[3] V. Jacobson, "Congestion avoidance and control," in *Proc. 1988 SIGCOMM*,pp. 314–329.
[4] V. Jacobson, "Modified TCP congestion avoidance algorithm," Apr.1990.
[5] K. K. Ramakrishnan and S. Floyd, "Proposals to add explicit congestion notification (ECN) to IP," RFC 2481, Jan. 1999.
[6] D. Katabi, M. Handley, and C. Rohrs, "Congestion control for high bandwidth-delay product networks," in *Proc. 2002 SIGCOMM*, pp. 89–102.
[7] S.H.Low,F.Paganini,J.Wang,*et al.*, "Dynamics of TCP/AQM and a scalable control," in *Proc. 2002 IEEE INFOCOM*, vol. 1, pp. 239–248.
[8] S. Floyd, "High-speed TCP for large congestion windows," RFC 3649, Dec. 2003.
[9] W. Feng and S. Vanichpun, "Enabling compatibility between TCP Reno and TCP Vegas," in *Proc. 2003 Symp. Applications Internet*, pp. 301–308.
[10] M. M. Hassani and R. Berangi, "An analytical model for evaluating utilization of TCP Reno," in *Proc. 2007 Int. Conf. Computer Syst.Technologies*, p. 14-1-7.
[11] N. Dukkipati, N. McKeown, and A. G. Fraser, "RCP-AC congestion control to make flows complete quickly in any environment," in *Proc.2006 IEEE INFOCOM*, pp. 1–5.
[12] Y. Zhang, D. Leonard, and D. Loguinov, "JetMax: scalable max-min congestion control for high-speed heterogeneous networks," in *Proc.2006 IEEE INFOCOM*, pp. 1–13.
[13] B. Wydrowski, L. Andrew, and M. Zukerman, "MaxNet: a congestion control architecture for scalable networks," *IEEE Commun. Lett.*,vol.7, no. 10, pp. 511–513, Oct. 2003.
[14] Y. Zhang and M. Ahmed, "A control theoretic analysis of XCP," in *Proc.2005 IEEE INFOCOM*, vol. 4, pp. 2831–2835.
[15] Y. Zhang and T. R. Henderson, "An implementation and experimental study of the explicit control protocol (XCP)," in *Proc. 2005 IEEEINFOCOM*, vol. 2, pp. 1037–1048.
[16] J. Pu and M. Hamdi, "Enhancements on router-assisted congestion control for wireless networks," *IEEE Trans. Wireless Commun.*,vol.7, no. 6, pp. 2253–2260, June 2008.
[17] F. Abrantes, J. Araujo, and M. Ricardo, "Explicit congestion control algorithms for time varying capapcity media," *IEEE Trans. Mobile Comput.*, vol. 10, no. 1, pp. 81–93, Jan. 2011.
[18] L. Benmohamed and S. M. Meerkov, "Feedback control of congestion in packet switching networks: the case of a single congested node,"*IEEE/ACM Trans. Netw.*, vol. 1, no. 6, pp. 693–708, Dec. 1993.
[19] Y. Hong and O. Yang, "Design of adaptive PI rate controller for besteffort traffic in the Internet based on phase margin," *IEEE Trans. Parallel Distrib. Syst.*, vol. 18, no. 4, pp. 550–561, 2007.[20] W. Hu and G. Xiao, "Design of congestion control based on instantaneous queue size in the routers," in *Proc. 2009 IEEE GLOBECOM*, pp. 1–6.
[21] S. Chong, S. Lee, and S. Kang, "A simple, scalable, and stable explicit rate allocation algorithm for max-min flow control with minimum rate guarantee," *IEEE/ACM Trans. Netw.*, vol. 9, no. 3, pp. 322–335, June 2001.
[22] Y. Hong and O. Yang, "An API-RCP design using pole placement technique," in *Proc. 2011 IEEE ICC*, pp. 1–5.
[23] B. Ribeiro, T. Ye, and D. Towsley, "Resource-minimalist flow size histogram estimator," in *Proc. 2008 ACM SIGCOMM Conf. Internet Measurement*, pp. 285–290.
[24] Y. H. Long, T. K. Ho, and A. B. Rad, "An enhanced explicit rate algorithm for ABR traffic control in ATM networks," *Int. J. Commun. Syst*, vol. 14, pp. 909–923, 2011.
[25] L. Roberts, "Enhanced PRCA proportional rate control algorithm," AFTM-R, Aug. 1994.
[26] S. J. Lee and C. L. Hou, "A neural-fuzzy system for congestion control in ATM networks," *IEEE Trans. Syst. Man Cybern. B., Cybern.*,vol.30, no. 1, pp. 2–9, 2000.
[27] A. Vashist, M. Siun-Chuon, A. Poylisher, *et al.*, "Leveraging social network for predicting demand and estimating available resources for communication network management," in *Proc. 2011 IEEE/IFIP Int. Symp. Integrated Netw. Manage.*, pp. 547–554.
[28] D. Toelle and R. Knorr, "Congestion control for carrier ethernet using network potential," *Proc. 2006 IEEE/IFIP Netw. Operations Manage. Symp.*, pp.1–4.
[29] Y. Yan, A. El-Atawy, and E. Al-Shaer, "A game-theoretic model for capacity-constrained fair bandwidth allocation," *Int. J. Netw. Manage.*, vol. 18, no. 6, pp. 485–504, Nov. 2008.
[30] M. Charalambides, P. Flegkas, G. Pavlou, *et al.*, "Policy conflict analysis for diffserv quality of service management," *IEEE Trans. Netw. Service Manage.*, vol. 6, no. 1, pp. 15–30, Mar. 2009.
[31] G. Pavlou, "Traffic engineering and quality of service management for IP-based NGNs," in *Proc. 2006 IEEE/IFIP Netw. Operations Manage. Symp.*, p. 589.
[32] D. Chalmers and M. Sloman, "A survey of quality of service in mobile computing environments," *IEEE Commun. Surveys & Tutorials*,vol.2, no. 2, pp. 2–10, 1999.
[33] G. Kesidis, "Congestion control alternatives for residential broadband access," *Proc. 2010 IEEE Netw. Operations Manage. Symp.*, pp. 874–877.
[34] J. Wang and V. Leung, "Incentive engineering at congested wireless access points using an integrated multiple time scale control mechanism," in *Proc. 2006 IEEE/IFIP IEEE Netw. Operations Manage. Symp.*, pp. 1–4.
[35] S. Secci, M. Huaiyuan, B. Helvik, and J. Rougier, "Resilient inter-carrier traffic engineering for Internet peering interconnections," *IEEE Trans. Netw. Service Manage.*, vol. 8, no. 4, pp. 274–284, 2011.
[36] K. M. Passino and S. Yurkovich, *Fuzzy Control*.AddisonWesley Longman Inc., 1998.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 9, September 2014

[37] E. Jammeh, M. Fleury, C. Wagner, *et al.*, "Interval type-2 fuzzy logic congestion control for video streaming across IP networks," *IEEE Trans.Fuzzy Syst.*, vol. 17, no. 5, pp. 1123–1142, 2009.
[38] T. W. Vaneck, "Fuzzy guidance controller for an autonomous boat," *IEEE Control Syst. Mag.*, vol. 17, no. 2, pp. 43–51, Apr. 1997.
[39] T. Kiryu, I. Sasaki, K. Shibai, *et al.*, "Providing appropriate exercise levels for the elderly," *IEEE Eng. Med. Biol. Mag.*, vol. 20, no. 6, pp.116–124, 2001.
[40] C. Chang and R. Cheng, "Traffic control in an ATM network using fuzzy set theory," in *Proc. 1994 IEEE INFOCOM*, vol. 3. pp. 1200–1207.
[41] J. Harju and K. Pulakka, "Optimization of the performance of a ratebased congestion control system by using fuzzy controllers," in *Proc.1999 IEEE IPCCC*, pp. 192–198.
[42] R. Chang and C. Cheng, "Design of fuzzy traffic controller for ATM networks," *IEEE/ACM Trans. Netw.*, vol. 4, no. 3, pp. 460–469, June 1996.
[43] H. Aoul, A. Nafaa, D. Negru, and A. Mehaoua, "FAFC: fast adaptive fuzzy AQM controller for TCP/IP networks," in *Proc. 2004 IEEE GLOBECOM*, vol. 3, pp. 1319–1323.
[44] C. Chrysostomou, A. Pitsillides, G. Hadjipollas, *et al.*, "Fuzzy explicit marking for congestion control in differentiated services networks," in*Proc. 2003 IEEE Int. Symp. Computers Commun.*, vol. 1, pp. 312–319.
[45] S. Kaehler. Available: http://www.seattlerobotics.org/encoder/mar98/fuz/ flindex.html
[46] H. Ying, W. Siler, and J. J. Buckley, "Fuzzy control theory: a nonlinear case," *Automatica*, vol. 26, no. 3, pp. 513–520, 1990.
[47] H. Jiang and C. Dovrolis, "Passive estimation of round-trip times," *ACM SIGCOMM Computer Commun. Rev.*, vol. 32, no. 3, 2002.
[48] Available: http://www.icir.org/floyd/ccmeasure.html
[49] R. C. Dorf and R. H. Bishop, *Modern Control Systems*, 11th edition. Pearson Prentice Hall, 2008.
[50] M. E. Crovella and A. Bestavros, "Self-similarity in world wide web traffic: evidence and possible causes," *IEEE/ACM Trans. Netw.*,vol.5, no. 6, pp. 835–846, Dec. 1997.
[51] "OPNET modeler manuals," OPNET version 11.5, OPNET Technologies Inc., 2005.
[52] D. Gross, J. Shortle, J. Thompson, *et al., Fundamentals of Queueing Theory*, 4th edition. John Wiley & Sons Inc., 2008.
[53] J. Liu and O. Yang, "Stability analysis and evaluation of the IntelRate controller for high-speed heterogeneous networks," in *Proc. 2011 IEEE*